TREND MICRO™

3.0

TREND MICRO™ Smart Protection Server

Manual del administrador

Seguridad más inteligente

Endpoint Security

Messaging Security

Protected Cloud

Web Security

Trend Micro Incorporated se reserva el derecho de efectuar cambios en este documento y en los productos o servicios que en él se describen sin previo aviso. Antes de instalar y empezar a utilizar el producto o servicio, consulte los archivos Léame, las notas de la versión o la última versión de la documentación pertinente, que se encuentra disponible en el sitio Web de Trend Micro, en:

http://docs.trendmicro.com/es-es/home.aspx

Trend Micro, el logotipo en forma de pelota de Trend Micro, TrendLabs, OfficeScan y Smart Protection Network son marcas registradas o marcas comerciales de Trend Micro Incorporated. El resto de nombres de productos o empresas pueden ser marcas comerciales o marcas comerciales registradas de sus respectivos propietarios.

Copyright © 2014 Trend Micro Incorporated. Reservados todos los derechos.

Nº de documento: APEM36294/140116

Fecha de publicación: marzo de 2014

Protegido por las patentes de Estados Unidos: Patentes pendientes

Esta documentación presenta las características principales del producto o servicio o proporciona instrucciones de instalación para un entorno de producción. Antes de instalar o utilizar el producto o servicio, es importante que la lea.

Se puede encontrar información detallada acerca de cómo utilizar características específicas del producto o servicio en el Centro de Ayuda en línea de Trend Micro o en la Base de conocimientos de Trend Micro.

Trend Micro trata constantemente de mejorar la documentación. Si tiene alguna duda, comentario o sugerencia con relación a los documentos de Trend Micro, póngase en contacto con nosotros a través del correo electrónico docs@trendmicro.com.

Puede valorar la documentación en el siguiente sitio Web:

http://www.trendmicro.com/download/documentation/rating.asp

Tabla de contenidos

Prefacio

Prefacio v

Acerca de Trend Micro vi

Documentación del producto vi

Audience vi

Convenciones del documento vii

Capítulo 1: Introducción

¿Cómo funciona el Servidor de protección inteligente de Trend Micro? 1-2

- Una nueva solución necesaria 1-2
- Soluciones de la Red de Protección Inteligente 1-3

Novedades de esta versión 1-8

Funciones y ventajas principales 1-10

Red de Protección Inteligente de Trend Micro 1-11

- Servicios de File Reputation 1-12
- Servicios de Reputación Web 1-12
- Smart Feedback 1-13

Capítulo 2: Usar el servidor de protección inteligente

Usar la consola del producto 2-2

- Acceder a la consola del producto 2-3

Usar Smart Protection 2-3

- Uso de los servicios de reputación 2-3
- Configurar las listas de URL permitidas y bloqueadas 2-6
- Configurar servicios de alerta de contacto de C&C 2-7
- Activar Smart Feedback 2-9

Actualizaciones 2-10

- Configurar actualizaciones manuales 2-10

Configurar actualizaciones programadas 2-10
Actualizaciones de archivos de patrones 2-11
Actualizaciones de archivos de programa 2-11
Configurar una fuente de actualización 2-15

Tareas administrativas 2-15
Servicio SNMP 2-15
Configuración del proxy 2-21
Asistencia 2-23

Cambiar la contraseña de la consola de producto 2-23

Capítulo 3: Supervisión de Smart Protection Server

Uso de la pantalla Resumen 3-2
Pestañas 3-3
Componentes 3-6

Registros 3-14
Registro de acceso Web bloqueado 3-14
Registro de actualización 3-16
Registro de servicios de reputación 3-16
Mantenimiento de los registros 3-17

Notificaciones 3-18
Notificaciones por correo electrónico 3-18
Notificaciones mediante captura SNMP 3-21

Capítulo 4: Obtener ayuda

Uso del portal de asistencia 4-2
Problemas conocidos 4-2
Archivos hotfix, parches y service packs 4-3

Enciclopedia de amenazas 4-3

Ponerse en contacto con Trend Micro 4-4
Agilizar la llamada al servicio de asistencia 4-5

TrendLabs 4-5

Apéndice A: Comandos de la Interfaz de línea de comandos (CLI)

Apéndice B: Glosario

Índice

Índice IN-1

Prefacio

Prefacio

Bienvenido a Smart Protection Server™ Manual del administrador. Este documento contiene información sobre la configuración del producto.

Los temas que se incluyen son:

- *Acerca de Trend Micro en la página vi*
- *Documentación del producto en la página vi*
- *Audience en la página vi*
- *Convenciones del documento en la página vii*

Acerca de Trend Micro

Trend Micro Incorporated ofrece software y servicios de protección antivirus, antispam y filtrado de contenidos. Trend Micro ayuda a clientes de todo el mundo a impedir que el código malicioso dañe sus equipos.

Documentación del producto

La documentación del Servidor de Protección Inteligente se compone de los siguientes elementos:

DOCUMENTACIÓN	DESCRIPCIÓN
Manual de instalación y actualización	le ayuda a planificar la instalación, las actualizaciones y la implementación.
Manual del administrador	le ayuda a establecer la configuración de todos los productos.
Ayuda en línea	proporciona instrucciones detalladas acerca de cada archivo y cómo configurar todas las funciones a través de la interfaz de usuario.
Archivo Léame	contiene la última información de productos que puede no encontrarse en otra documentación. Entre sus temas se incluyen: una descripción de las funciones, consejos para la instalación, problemas conocidos y el historial de versiones del producto.

La documentación está disponible en:

http://downloadcenter.trendmicro.com/?regs=ES

Audience

La documentación de Smart Protection Server™ está destinada a administradores y gestores de TI. Presupone que el lector cuenta con conocimientos en profundidad sobre redes.

Pero no presupone que el lector tenga conocimiento alguno sobre la tecnología de prevención de virus o malware, o antispam.

Convenciones del documento

El Manual del usuario de Smart Protection Server™ utiliza las siguientes convenciones.

TABLA 1. Convenciones del documento

CONVENCIÓN	DESCRIPCIÓN
TODO EN MAYÚSCULAS	Acrónimos, abreviaciones y nombres de determinados comandos y teclas del teclado
Negrita	Menús y comandos de menú, botones de comandos, pestañas y opciones
Navegación > **Ruta**	La ruta de navegación a una determinada pantalla. Por ejemplo, **Archivo** > **Guardar** significa hacer clic en **Archivo** y, a continuación, en **Guardar** en la interfaz.
Nota	Notas sobre la configuración
Consejo	Recomendaciones o sugerencias
¡ADVERTENCIA!	Acciones críticas y opciones de configuración

Capítulo 1

Introducción

En este capítulo se presentan y describen las características de Trend Micro™ Smart Protection Server™.

Los temas que se incluyen son:

- *¿Cómo funciona el Servidor de protección inteligente de Trend Micro? en la página 1-2*
- *Novedades de esta versión en la página 1-8*
- *Funciones y ventajas principales en la página 1-10*
- *Red de Protección Inteligente de Trend Micro en la página 1-11*

¿Cómo funciona el Servidor de protección inteligente de Trend Micro?

Trend Micro™ Smart Protection Server™ es una solución de protección avanzada de última generación basada en Internet. La base de esta solución es una arquitectura de exploración avanzada que aprovecha las firmas de prevención de malware que se almacenan en Internet.

Esta solución aprovecha la tecnología de File Reputation y reputación Web para detectar los riesgos para la seguridad. Esta tecnología funciona redireccionando un gran número de listas y firmas de prevención de malware que se han almacenado previamente en los puntos finales a Trend Micro Smart Protection Server.

Al utilizar este enfoque, se reduce considerablemente el impacto en el sistema y en la red del siempre creciente volumen de actualizaciones de firmas en el punto final.

Una nueva solución necesaria

En este enfoque de gestión de amenazas basada en archivos, la mayor parte de los patrones (o definiciones) que se necesitan para proteger un punto final se envían según una programación sistemática. Estos patrones se envían por lotes desde Trend Micro a los puntos finales. Cuando se recibe una nueva actualización, el software de prevención de virus o malware del punto final vuelve a leer el lote de definiciones de patrones de los riesgos de virus o malware nuevos de la memoria. Si aparece un riesgo de virus o malware nuevo, el patrón tiene que ser actualizado de nuevo de forma parcial o completa y se vuelve a leer en el punto final para garantizar una protección continuada.

A medida que ha ido pasando el tiempo, ha aumentado significativamente el volumen de amenazas emergentes exclusivas. Se espera que este volumen de amenazas siga creciendo casi exponencialmente en los próximos años. Esto es una tasa de crecimiento que supera con creces el volumen de los riesgos de seguridad conocidos actualmente. Aún más, el volumen de los riesgos de seguridad representa un nuevo tipo de riesgo de seguridad. El volumen de los riesgos de seguridad puede tener un impacto negativo en el rendimiento de los servidores y estaciones de trabajo, en el uso del ancho de banda de red y, en general, en el tiempo que se tarda en proporcionar una protección de calidad, o "tiempo para la protección".

Trend Micro ha sido pionero en un enfoque nuevo para gestionar el volumen de amenazas que se centra en hacer a los clientes de Trend Micro inmunes a esta amenaza que representa el volumen de virus o malware. La tecnología y la arquitectura que se utiliza en este esfuerzo pionero aprovecha la tecnología de redireccionamiento del almacenamiento de firmas y patrones de virus o malware a Internet. Mediante el redireccionamiento del almacenamiento de estas firmas de virus o malware a Internet, Trend Micro puede proporcionar mejor protección a sus clientes frente al futuro volumen de riesgos de seguridad emergentes.

Soluciones de la Red de Protección Inteligente

El proceso de consulta basado en Internet utiliza dos tecnologías basadas en red:

- Trend Micro™ Smart Protection Network™: una infraestructura basada en Internet y reducida de forma global que proporciona servicios a los usuarios que no dispongan de acceso inmediato a la red de empresa.
- Servidor de Protección Inteligente: Smart Protection Server existe en la red local. Están disponibles para los usuarios que tengan acceso a la red de empresa local. Estos servidores locales están diseñados para localizar las operaciones de la red de empresa y optimizar su eficiencia.

Nota

Instale varios Servidores de Protección Inteligente para garantizar una protección continuada en el caso de que no esté disponible la conexión a un Servidor de Protección Inteligente.

Estos dos nuevos productos basados en la red alojan la mayoría de las definiciones de patrones de virus o malware y las puntuaciones de reputación Web. Trend Micro™ Smart Protection Network™ y Smart Protection Server ponen estas definiciones a disposición de otros puntos finales de la red para comprobar si existen posibles amenazas. Las consultas sólo se envían a los Servidores de Protección Inteligente si el punto final no puede determinar el riesgo del archivo o la URL.

Los puntos finales cuentan con tecnología File Reputation y Reputación Web para realizar las consultas a los Servidores de Protección Inteligente de Trend Micro como parte de sus actividades habituales de protección de sistemas. En esta solución, los agentes envían información de identificación, que determina la tecnología de Trend

Micro, a los Servidores de Protección Inteligente para las consultas. Los agentes nunca envían el archivo completo cuando utilizan tecnología File Reputation. El riesgo del archivo se determina mediante la información de identificación.

Archivos de patrones

El proceso de consulta basado en Internet utiliza un pequeño archivo de patrones local junto con un sistema de consultas en Internet en tiempo real. El sistema de consultas por Internet comprueba los archivos, las direcciones URL y demás componentes con un Servidor de Protección Inteligente durante el proceso de verificación. Los Servidores de Protección Inteligente utilizan varios algoritmos para garantizar un proceso eficiente que utiliza el mínimo de ancho de banda de red.

Hay tres archivos de patrón:

- **Smart Scan Pattern**: este patrón se descarga y está disponible en los Servidores de Protección Inteligente y la Red de Protección Inteligente de Trend Micro. Se actualiza cada hora.
- **Smart Scan Agent Pattern**: este patrón se almacena localmente en el punto final para las exploraciones que no necesitan los Servidores de Protección Inteligente. Se actualiza todos los días.
- **Lista de Bloqueo Web**: los Servidores de Protección Inteligente descargan este patrón de los servidores ActiveUpdate de Trend Micro. Este patrón se utiliza para las consultas de Reputación Web.

Proceso de actualización de patrones

Las actualizaciones de los patrones son una respuesta a las amenazas de seguridad. La Red de Protección Inteligente y los Servidores de Protección Inteligente descargan el archivo Smart Scan Pattern de los servidores ActiveUpdate. Los productos de Trend Micro que son compatibles con los Servidores de Protección Inteligente descargan Smart Scan Agent Patterns de los servidores ActiveUpdate.

Los puntos finales del interior de su intranet descargan archivos Smart Scan Agent Pattern desde los productos de Trend Micro que son compatibles con los Servidores de Protección Inteligente. Los puntos finales externos son puntos finales que se encuentran fuera de la intranet y no pueden conectarse a los Servidores de Protección Inteligente o a

los productos de Trend Micro que son compatibles con los Servidores de Protección Inteligente.

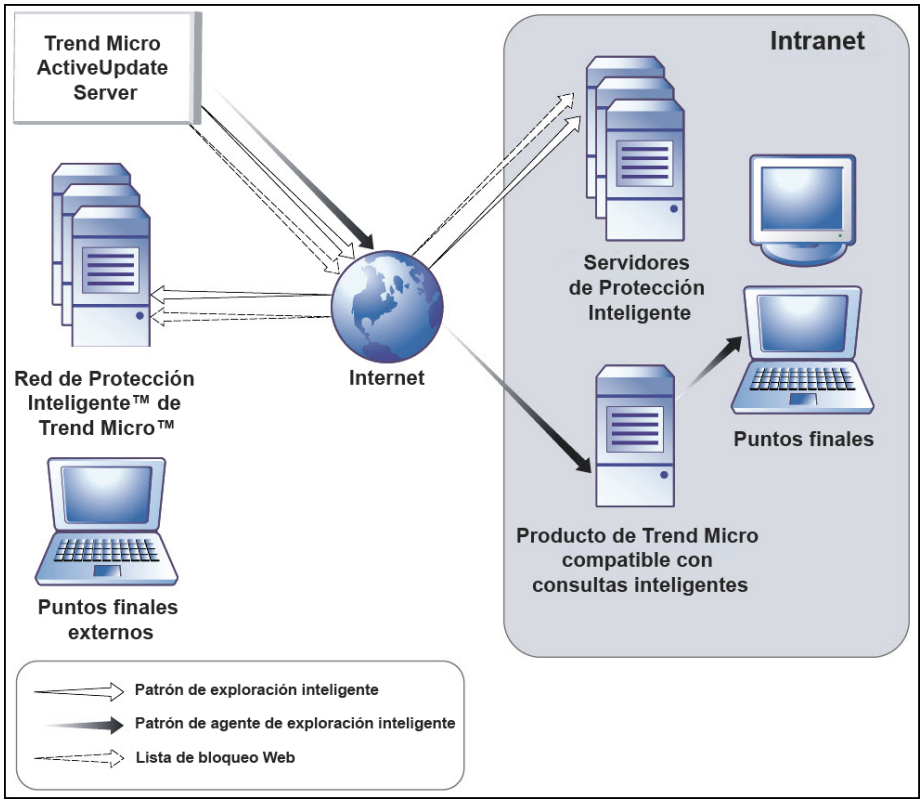

Trend Micro ActiveUpdate Server
Intranet
Servidores de Protección Inteligente
Red de Protección Inteligente™ de Trend Micro™
Internet
Puntos finales
Puntos finales externos
Producto de Trend Micro compatible con consultas inteligentes
Patrón de exploración inteligente
Patrón de agente de exploración inteligente
Lista de bloqueo Web

FIGURA 1-1. Proceso de actualización de patrones

El proceso de consulta

Los puntos finales que haya actualmente en la intranet utilizan los Servidores de Protección Inteligente para realizar consultas. Los puntos finales que no estén actualmente en la intranet se pueden conectar a la Red de Protección Inteligente de Trend Micro para realizar consultas.

A pesar de que es necesaria la conexión a la red para utilizar los Servidores de Protección Inteligente, los puntos finales que no dispongan de acceso a la red aún pueden beneficiarse de la tecnología de Trend Micro. Smart Scan Agent Pattern y la tecnología de exploración que hay en los puntos finales protege a los puntos finales que no tienen acceso a una conexión a la red.

Los agentes instalados en los puntos finales primero realizan una exploración del punto final. Si el agente no puede determinar el riesgo del archivo o la URL, puede verificar este riesgo enviando una consulta a un Servidor de Protección Inteligente.

TABLA 1-1. Comportamientos de protección basados en el acceso a la intranet

LOCALIZACIÓN	ARCHIVO DE PATRONES Y COMPORTAMIENTO DE CONSULTA
Acceso a la intranet	• **Archivos de patrones**: los puntos finales descargan el archivo Smart Scan Agent Pattern desde los productos de Trend Micro que sean compatibles con los Servidores de Protección Inteligente. • **Consultas**: los puntos finales se conectan al Servidor de Protección Inteligente para realizar consultas.
Si acceso a la intranet	• **Archivos de patrones**: los puntos finales no descargan el archivo Smart Scan Agent Pattern más reciente si no hay disponible una conexión a un producto de Trend Micro que sea compatible con los Servidores de Protección Inteligente. • **Consultas**: los puntos finales exploran los archivos con recursos locales como el archivo Smart Scan Agent Pattern.

La tecnología avanzada de filtrado permite al agente "almacenar en caché" el resultado de la consulta. De esta manera se mejora el rendimiento de exploración y se elimina el tener que enviar la misma consulta a los Servidores de Protección Inteligente más de una vez.

Un agente que no pueda comprobar el riesgo de un archivo de forma local y que no pueda conectarse a ningún servidor de Smart Protection Server después de varios intentos, marca el archivo para su verificación y permite acceder a él de forma temporal. Cuando se restaure la conexión con un servidor de protección inteligente, todos los archivos marcados se volverán a explorar. Entonces, se realizará una acción de exploración en los archivos que se confirmen como una amenaza para su red.

Consejo

Instale varios Servidores de Protección Inteligente para garantizar una protección continuada en el caso de que no esté disponible la conexión a un Servidor de Protección Inteligente.

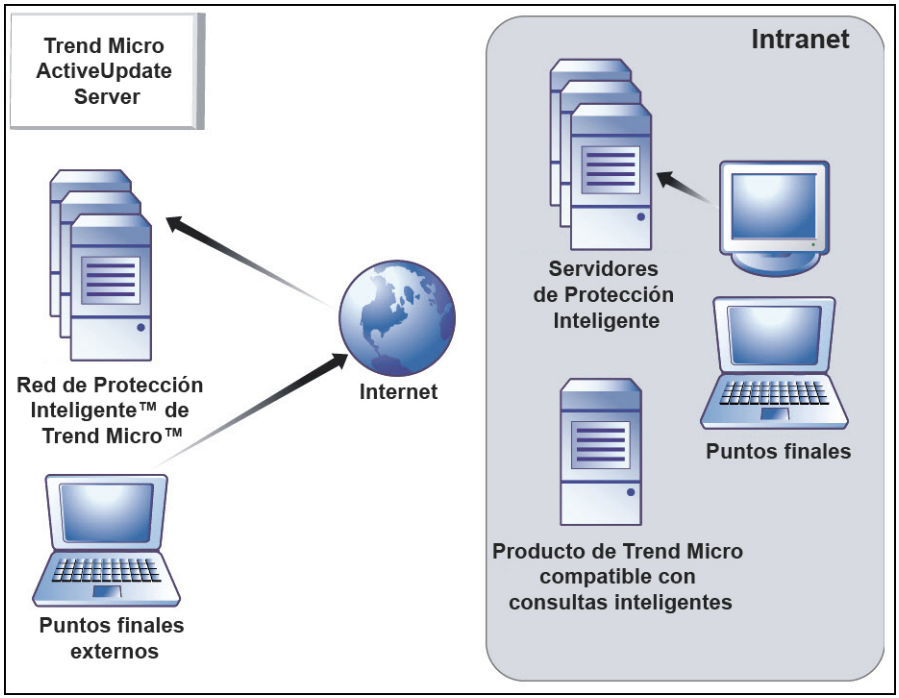


FIGURA 1-2. Proceso de consulta

Novedades de esta versión

Trend Micro™ Smart Protection Server™ incluye las siguientes nuevas funciones y mejoras:

TABLA 1-2. Nuevo en la versión 3.0

CARACTERÍSTICA	DESCRIPCIÓN
Rendimiento mejorado del patrón	Se ha mejorado el rendimiento de los Servicios de Reputación Web y de File Reputation con el fin de reducir el uso de los recursos de memoria al cargar los patrones. • Servicios de Reputación Web Se han mejorado los Servicios de Reputación Web para permitir actualizaciones incrementales de la Lista de bloqueo Web. De esta forma se reduce la memoria y el uso del ancho de banda de red al cargar la Lista de bloqueo Web. • Servicios de File Reputation Se ha mejorado el mecanismo de importación del registro de los Servicios de File Reputation para actualizar la base de datos directamente desde el servidor Web. Con esto, es posible garantizar lo siguiente: • La importación de los registros de acceso en la base de datos es ahora en tiempo real, además se tarda menos tiempo en procesar la misma cantidad de datos y se mejora el rendimiento de E/S del disco. • Reducción de la carga del servidor y del uso de recursos.
Capacidad mejorada	Un servidor de Smart Protection Server independiente admite ahora hasta 25.000 agentes de Trend Micro™ OfficeScan™ 11.

CARACTERÍSTICA	DESCRIPCIÓN
Mejora de panel	• Proporciona nuevos diseños y tablas para componentes. • Los componentes obtienen ahora los datos del servidor Web diariamente. • Problemas de tiempo de espera fijo y otros errores menores.
Nueva base de información de administración (MIB) para la información del sistema	Se proporciona la posibilidad de consultar la información del sistema de Smart Protection Server directamente desde una herramienta de explorador MIB de terceros. Estas son: • SNMP MIB-2 System (1.3.6.1.2.1.1) • SNMP MIB-2 Interfaces (1.3.6.1.2.1.2) Para obtener más información, consulte *MIB admitido en la página 2-20*.
Nuevo comando de la Interfaz de línea de comandos (CLI)	Se proporcionan nuevos comandos para: • Configurar un servidor NTP (`configure ntp`) • Cambiar el puerto de servicio (`configure port`) **Importante** Utilice este comando solo si hay algún conflicto con el puerto de servicio actual. Para obtener más información, consulte *Comandos de la Interfaz de línea de comandos (CLI) en la página A-1*.
Se han mejorado las capacidades de la máquina virtual.	• Smart Protection Server admite ahora adaptadores de red VMware VMXNET 3 en un entorno IPv6. • Se ha solucionado el problema con el adaptador de red IPv6 Microsoft Hyper-V con Linux Kernel versión 5.8.

TABLA 1-3. Nuevo en la revisión 1 de la versión 2.6

CARACTERÍSTICA	DESCRIPCIÓN
Integración con el servidor de Deep Discovery Advisor y la lista Virtual Analyzer	Los servidores de Smart Protection Server se pueden integrar con Deep Discovery Advisor para obtener la lista de servidores de C&C de Virtual Analyzer. Virtual Analyzer de Deep Discovery Advisor evalúa los riesgos potenciales en un entorno seguro y, mediante el uso de métodos avanzados de comprobación heurísticos y de comportamiento, asigna un nivel de riesgo a las amenazas analizadas. Virtual Analyzer rellena la lista Virtual Analyzer con cualquier amenaza que intente conectarse a un posible servidor de C&C. La lista Virtual Analyzer está muy enfocada a cada empresa y proporciona una defensa más personalizada ante los ataques con destino. Los servidores de Smart Protection Server recuperan la lista de Deep Discovery Advisor y, de este modo, puede comparar todas las posibles amenazas de C&C tanto con la lista de inteligencia global como con la lista de Virtual Analyzer local.

TABLA 1-4. Nuevo en la versión 2,6

CARACTERÍSTICA	DESCRIPCIÓN
Mejora de panel	Ya se puede mostrar el panel en aquellos dispositivos que no son compatibles con Adobe™ Flash™ Player.
Solución de algunos problemas menores	Trend Micro ha solucionado algunos problemas menores.

Funciones y ventajas principales

Trend Micro Smart Protection Server proporciona las siguientes características y ventajas:

- Tecnología File Reputation
  - La red de empresa se encontrará así en una mejor posición para gestionar la amenaza que supone el volumen.

- El "tiempo para proteger" frente a las amenazas emergentes disminuye considerablemente.
- El consumo de la memoria del kernel en las estaciones de trabajo se reduce de forma considerable y con el tiempo aumenta mínimamente.
- Mejora la administración y simplifica la gestión. El grueso de actualizaciones de las definiciones de patrones sólo se tiene que entregar a un servidor en lugar de a varias estaciones de trabajo. De esta manera, se reduce el grueso del impacto de una actualización de patrones en varias estaciones de trabajo.
- Protege frente a ataques basados en la Web y combinados.
- Detiene virus o malware, troyanos, gusanos y más variantes nuevas de estos riesgos de seguridad.
- Detecta y elimina spyware o grayware (incluidos los rootkits ocultos).

- Tecnología de Reputación Web
  - Protege frente a ataques basados en la Web y combinados.
  - Los clientes preocupados por la privacidad no deben tener miedo de revelar información confidencial a Red de Protección Inteligente a través de las consultas de Reputación Web.
  - El tiempo de respuesta del Servidor de Protección Inteligente a las consultas se reduce en comparación con las consultas a la Red de Protección Inteligente.
  - Al instalar un Servidor de Protección Inteligente en la red se reduce la carga del ancho de banda de gateway.

Red de Protección Inteligente de Trend Micro

Trend Micro™ Smart Protection Network™ es una infraestructura de seguridad de contenidos de clientes por Internet de última generación diseñada para proteger a los clientes de los riesgos de seguridad y las amenazas Web. Facilita que las soluciones locales y las alojadas protejan a los usuarios cuando están en red, en casa o en movimiento, utilizando para ello agentes ligeros para acceder a su correlación de correo

electrónico de Internet única, a las tecnologías de File Reputation y reputación Web y a las bases de datos de amenazas. La protección de los clientes se actualiza automáticamente y se refuerza a medida que van accediendo a la red más productos, servicios y usuarios, creando un servicio de protección de supervisión de entorno en tiempo real.

Servicios de File Reputation

Los Servicios de File Reputation comprueban la reputación de cada archivo en una extensa base de datos en la nube. Como la información sobre malware se almacena en red, los usuarios pueden acceder a ella de forma inmediata. Las redes con contenido de alto rendimiento y los servidores locales guardados en caché garantizan una latencia mínima durante el proceso de comprobación. La estructura en red ofrece una protección más inmediata y elimina la carga de la implementación de patrones, además de reducir de forma significativa el tamaño global del cliente.

Servicios de Reputación Web

Con una de las bases de datos de dominios y reputaciones más grandes del mundo, la tecnología de reputación Web de Trend Micro realiza un seguimiento de la credibilidad de los dominios Web mediante la asignación de un resultado de reputación basado en factores como la antigüedad del sitio Web, los cambios en la ubicación histórica y las indicaciones de actividades sospechosas descubiertas mediante el análisis de comportamientos malintencionados. A continuación seguirá con la exploración de los sitios y el bloqueo del acceso de los usuarios a los sitios infectados. Las funciones de la reputación Web garantizan que las páginas a las que accede el usuario son seguras y no contienen amenazas Web, como malware, spyware y fraudes de phishing que tienen como objetivo engañar al usuario para que proporcione información personal. Para aumentar la precisión y reducir los falsos positivos, la tecnología de reputación Web de Trend Micro asigna puntuaciones de reputación a páginas específicas dentro de los sitios en lugar de clasificar o bloquear sitios completos, ya que a veces son sólo partes de estos los que están afectados y las reputaciones pueden cambiar de forma dinámica con el tiempo.

Las funciones de la Reputación Web garantizan que las páginas Web a las que accede el usuario son seguras y no contienen amenazas Web, como malware, spyware y fraudes de phishing que tienen como objetivo engañar al usuario para que proporcione información

personal. La Reputación Web bloquea páginas Web en función de su clasificación de reputación. Cuando está activada, esta función ayuda a los usuarios a evitar URL maliciosas.

Smart Feedback

Trend Micro™ Smart Feedback proporciona una comunicación continua entre los productos Trend Micro, así como entre los centros de investigación de amenazas de la empresa y sus tecnologías, que ofrecen asistencia 24 horas al día, los 7 días de la semana. Cada nueva amenaza identificada mediante una simple verificación rutinaria de la reputación del cliente actualiza automáticamente todas las bases de datos de amenazas de Trend Micro, lo que bloquea cualquier encuentro posterior del cliente con dicha amenaza. Mediante el procesamiento continuo de la inteligencia de la amenaza, recopilada a través de su extensa red global de clientes y socios, Trend Micro ofrece protección automática en tiempo real frente a las amenazas más recientes y proporciona la seguridad "mejor juntos", que se asemeja a un tipo de vigilancia vecinal automatizado que involucra a la comunidad en la protección de los demás. La privacidad de la información personal o empresarial de un cliente está siempre protegida ya que la información recopilada sobre las amenazas está basada en la reputación de la fuente de comunicación, no en el contenido de la comunicación específica.

Capítulo 2

Usar el servidor de protección inteligente

En este capítulo se ofrece información sobre la configuración de Trend Micro™ Smart Protection Server™.

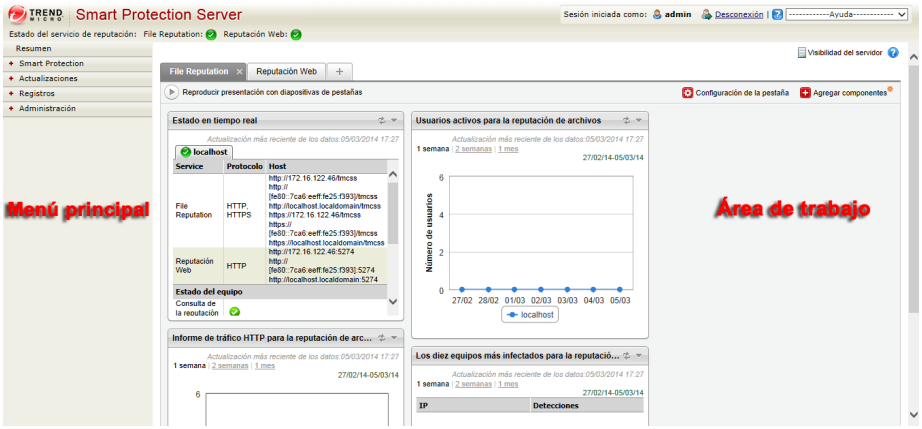
Los temas que se incluyen son:

- *Usar la consola del producto en la página 2-2*
- *Usar Smart Protection en la página 2-3*
- *Actualizaciones en la página 2-10*
- *Tareas administrativas en la página 2-15*
- *Configuración del proxy en la página 2-21*
- *Cambiar la contraseña de la consola de producto en la página 2-23*

Usar la consola del producto

La consola del producto consta de los siguientes elementos:

- **Menú principal**: proporciona enlaces a las pantallas **Resumen**, **Smart Protection**, **Actualizaciones**, **Registros** y **Administración**.
- **Área de trabajo**: vea aquí la información de resumen y el estado de los componentes, establezca la configuración, actualice los componentes y lleve a cabo tareas de administración.



Menú	Descripción
Resumen	Muestra información personalizada sobre los Servidores de Protección Inteligente, el tráfico y las detecciones al agregar complementos.
Smart Protection	Proporciona opciones para configurar los servicios de reputación, una Lista de URL permitidas/bloqueadas y Feedback Inteligente.
Actualizaciones	Proporciona opciones para configurar las actualizaciones programadas, las actualizaciones del programa manuales, las cargas de paquetes del programa y la fuente de actualización.

MENÚ	DESCRIPCIÓN
Registros	Ofrece opciones para realizar consultas en los registros y el mantenimiento de estos.
Administración	Ofrece opciones para configurar el servicio SNMP, las notificaciones, la configuración del proxy y recopilar información de diagnóstico para la solución de problemas.

Acceder a la consola del producto

Después de iniciar sesión en la consola Web, en la pantalla inicial se muestra el resumen de estado de los servidores de Smart Protection Server.

Procedimiento

1. Abra una ventana del explorador Web y escriba la URL que se indica tras la instalación en el banner de la CLI inicial.
2. Escriba, en los campos correspondientes, `admin` como nombre de usuario y la contraseña.
3. Haga clic en **Iniciar sesión**.

Usar Smart Protection

Esta versión de Smart Protection Server incluye los servicios de File Reputation y de Reputación Web.

Uso de los servicios de reputación

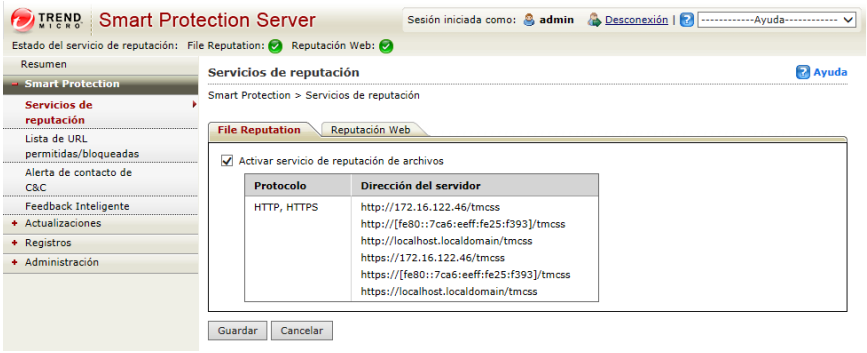
Active los servicios de reputación desde la consola del producto para permitir que otros productos de Trend Micro puedan utilizar la protección inteligente.

Activar los Servicios de File Reputation

Active los Servicios de File Reputation para permitir consultas desde los puntos finales.

Procedimiento

1. Vaya a **Smart Protection** > **Servicios de Reputación** y, a continuación, vaya a la pestaña **File Reputation**.



2. Seleccione la casilla de verificación **Activar el servicio de Reputación de Ficheros**.

3. Haga clic en **Guardar**.

   Ahora los demás productos de Trend Micro compatibles con los Servidores de Protección Inteligente pueden utilizar la dirección del servidor para las consultas de File Reputation.

Activar los Servicios de Reputación Web

Active los Servicios de Reputación Web para la compatibilidad con las consultas de URL desde los puntos finales. Estas son las opciones disponibles en esta pantalla.

- **Activar servicio de Reputación Web**: seleccione esta opción para admitir las consultas de Reputación Web de los puntos finales.

- **Dirección del servidor**: la utilizan otros productos de Trend Micro para las consultas de la Reputación Web.
- **Prioridad de filtrado**: seleccione esta opción para especificar la prioridad a la hora de filtrar las URL.

Procedimiento

1. Vaya a **Smart Protection** > **Servicios de Reputación** y, a continuación, vaya a la pestaña **Reputación Web**.

2. Seleccione la casilla de verificación **Activar servicio de reputación Web**.
3. (Opcional) Especifique la prioridad de la lista de URL permitidas y bloqueadas a la hora de filtrarlas.
4. Haga clic en **Guardar**.

   Ahora los demás productos de Trend Micro compatibles con Smart Protection Server pueden utilizar la dirección del servidor para las consultas de File Reputation.

Configurar las listas de URL permitidas y bloqueadas

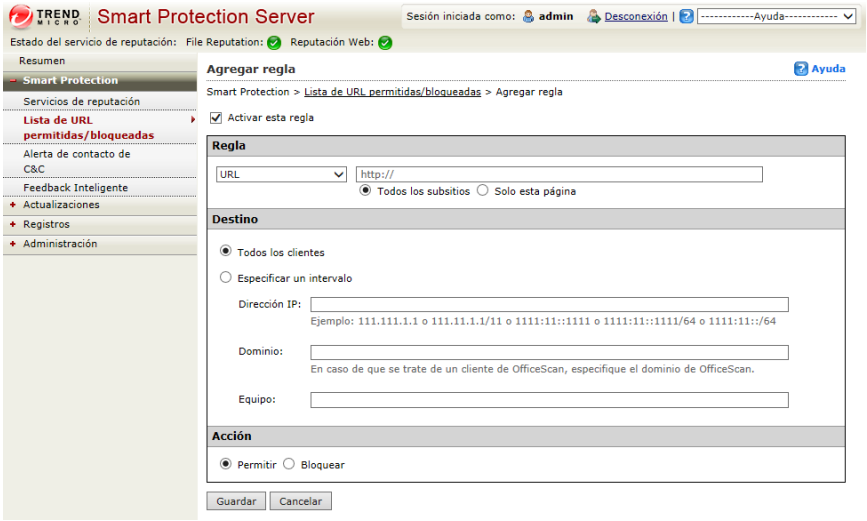
La Lista de URL permitidas/bloqueadas le permite especificar una lista personalizada de URL permitidas y/o bloqueadas. Esta lista se utiliza para la Reputación Web. Estas son las opciones disponibles en esta pantalla.

- **Buscar regla**: seleccione esta opción para buscar una cadena en la lista de reglas.
- **Probar URL**: seleccione esta opción para buscar reglas que activará la URL. La URL debe comenzar por `http://` o `https://`.

Procedimiento

1. Vaya a **Smart Protection** > **Lista de URL permitidas/bloqueadas**.
2. Haga clic en **Agregar**.

   Aparecerá la pantalla **Agregar regla**.



3. Seleccione la casilla de verificación **Activar esta regla**.
4. Seleccione una de las opciones siguientes:

- **URL**: para especificar una URL y aplicarla a todos los subsitios o sólo a una página.
- **URL con palabra clave**: para especificar una cadena y utilizar expresiones regulares.

Haga clic en **Probar** para ver los resultados de la aplicación de esta regla a las 20 URL más comunes y a las 100 URL principales del día anterior en el registro de acceso Web.

5. Seleccione una de las opciones siguientes:
   - **Todos los puntos finales**: para aplicarla a todos los puntos finales.
   - **Especificar un intervalo**: para aplicarla a un intervalo de direcciones IP, nombres de dominio y nombres de equipo.

   Nota
   Compatible con direcciones IPv4 e IPv6.

6. Seleccione **Permitir** o **Bloquear**.
7. Haga clic en **Guardar**.

Configurar servicios de alerta de contacto de C&C

Los Servicios de Command & Control (C&C) Contact Alert de Trend Micro proporcionan funciones mejoradas de detección y alerta para mitigar el daño que causan las amenazas continuas avanzadas y los ataques con destino. Los Servicios de C&C Contact Alert se integran con los Servicios de Reputación Web que determinan la acción que se va a realizar cuando se detectan direcciones de rellamada según el nivel de seguridad de la reputación Web.

Estas son las opciones disponibles en esta pantalla.

- **Servidor**: nombre del servidor o dirección IP del servidor de Deep Discovery Advisor, que proporciona la lista de C&C para análisis virtual.
- **Clave API**: clave API de Deep Discovery Advisor. Podrá encontrar la clave API en la página **Acerca de** en la consola Web de Deep Discovery Advisor.

- **Probar la conexión**: utilice este botón para comprobar que el nombre del servidor o la dirección IP del servidor, y la clave API de Deep Discovery Advisor sean correctos.
- **Registrar**: utilice este botón para registrar Smart Protection Server en Deep Discovery Advisor.
- **Eliminar el registro**: utilice este botón para eliminar el registro de Smart Protection Server de Deep Discovery Advisor.
- **Activar la lista de C&C para análisis virtual**: active esta opción para permitir que Smart Protection Server utilice la lista de C&C personalizada que ha analizado el servidor de Deep Discovery Advisor.
- **Sincronizar ahora**: utilice este botón para obtener de Deep Discovery Advisor una lista de C&C para análisis virtual actualizada.

Procedimiento

1. Escriba el nombre del servidor o la dirección IP del servidor de Deep Discovery Advisor.

   Nota

   El nombre del servidor es compatible con los formatos FQDN y la dirección IP es compatible con el formato IPv4.

2. Escriba la clave API.
3. Haga clic en **Registrar** para conectarse al servidor de Deep Discovery Advisor.

   Nota

   Los administradores pueden probar la conexión al servidor antes de registrarse en el servidor.

4. Seleccione **Activar lista de C&C para análisis virtual** para permitir que los servidores compatibles utilicen la lista de C&C personalizada que ha analizado el servidor local de Deep Discovery Advisor.

Nota

La opción **Activar la lista de C&C de Virtual Analyzer** solo está disponible una vez establecida correctamente la conexión al servidor de Deep Discovery Advisor.

5. Haga clic en **Guardar**.

Activar Smart Feedback

Trend Micro Smart Feedback comparte información anónima sobre amenazas con Trend Micro™ Smart Protection Network™, lo que permite a Trend Micro identificar y combatir rápidamente las nuevas amenazas. Puede desactivar la función de comentarios inteligentes en cualquier momento desde esta consola.

Procedimiento

1. Vaya a **Smart Protection** > **Smart Feedback**.

Nota

Asegúrese de que Smart Protection Server tenga conexión a Internet antes de activar Smart Feedback.

2. Seleccione **Activar Feedback Inteligente de Trend Micro**.

Smart Protection Server
Sesión iniciada como: admin
Desconexión
Ayuda
Estado del servicio de reputación:
File Reputation:
Reputación Web:
Resumen
Smart Protection
Servicios de reputación
Lista de URL permitidas/bloqueadas
Alerta de contacto de C&C
Feedback Inteligente
Actualizaciones
Registros
Administración
Feedback Inteligente
Smart Protection > Feedback Inteligente
TREND MICRO SMART PROTECTION NETWORK
Trend Micro Smart Protection Network es una infraestructura de seguridad Internet-cliente de última generación diseñada para ofrecer protección proactiva frente a las amenazas más recientes.
Más información
Feedback Inteligente
Cuando la función Trend Micro Smart Feedback está activada, ésta comparte información anónima sobre amenazas con Trend Micro Smart Protection Network, lo que permite a Trend Micro identificar y combatir rápidamente las nuevas amenazas. Puede desactivar la función de comentarios inteligentes en cualquier momento desde esta consola.
Activar la función de comentarios inteligentes de Trend Micro (recomendado)
Su sector (opcional):
Economía
Guardar
Cancelar

3. Seleccione el sector en el que opera.
4. Haga clic en **Guardar**.

Actualizaciones

La efectividad de Smart Protection Server depende del uso de los archivos de patrones y componentes más actualizados. Trend Micro lanza nuevas versiones de los archivos de Smart Scan Pattern cada hora.

Consejo

Trend Micro recomienda actualizar los componentes inmediatamente después de la instalación.

Configurar actualizaciones manuales

Puede realizar actualizaciones manuales de Smart Scan Pattern y la Lista de bloqueo Web.

Procedimiento

1. Vaya a **Actualizaciones**.
2. Haga clic en **Patrón** o en **Programa** en el menú desplegable.
3. Haga clic en **Actualizar ahora** o en **Guardar y actualizar ahora** para que se apliquen las actualizaciones de forma inmediata.

Configurar actualizaciones programadas

El Servidor de Protección Inteligente puede realizar actualizaciones programadas de Smart Scan Pattern y la Lista de bloqueo Web.

Procedimiento

1. Vaya a **Actualizaciones**.
2. Haga clic en **Patrón** o en **Programa** en el menú desplegable.
3. Especifique el programa de actualización.
4. Haga clic en **Guardar**.

Actualizaciones de archivos de patrones

Actualice los archivos de patrones para asegurarse de la última información se ha aplicado a las consultas. Estas son las opciones disponibles en esta pantalla:

- **Activar las actualizaciones programadas**: seleccione esta opción para configurar actualizaciones automáticas cada hora o cada 15 minutos.
- **Actualizar ahora**: haga clic para actualizar de inmediato todos los archivos de patrones.

Actualizaciones de archivos de programa

Actualice a la última versión del programa del producto para beneficiarse de las mejoras disponibles. Estas son las opciones disponibles en esta pantalla.

- **Sistema operativo**: seleccione esta opción para actualizar los componentes del sistema operativo.
- **Servidor de Protección Inteligente**: seleccione esta opción para actualizar el archivo de programa del servidor del producto.
- **Componentes**: seleccione esta opción para actualizar componentes.
- **Activar las actualizaciones programadas**: seleccione esta opción para actualizar los archivos del programa diariamente a una hora en concreto, o semanalmente.
- **Sólo descargar**: seleccione esta opción para descargar actualizaciones y que aparezca un aviso para actualizar archivos de programa.

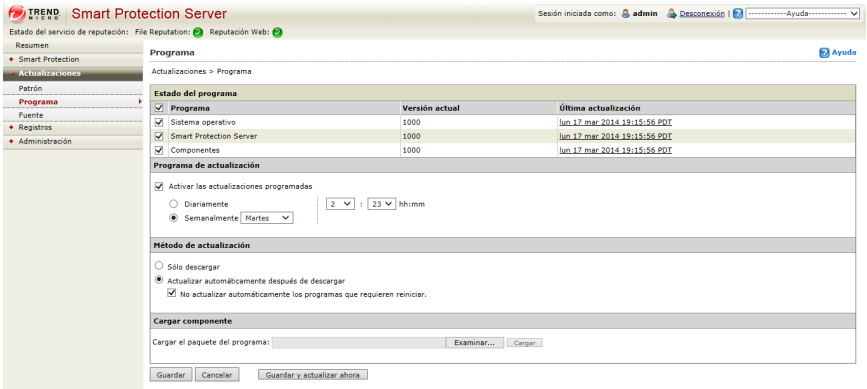
- **Actualizar automáticamente después de descargar**: seleccione esta opción para aplicar todas las actualizaciones al producto después de la descarga, independientemente de si se necesita o no reiniciar.
- **No actualizar automáticamente los programas que requieren reiniciar**: seleccione esta opción para descargar todas las actualizaciones y sólo instalar los programas que no requieren reiniciar.
- **Cargar**: haga clic en esta opción para cargar y actualizar un archivo de programa del Servidor de Protección Inteligente.
- **Examinar**: haga clic en esta opción para localizar un paquete de programa.
- **Guardar y actualizar ahora**: haga clic en esta opción para aplicar la configuración y realizar una actualización de forma inmediata.

Hay tres formas de actualizar el archivo del programa: actualizaciones programadas, actualizaciones manuales y cargar el componente.

Activar las actualizaciones programadas

Procedimiento

1. Vaya a **Actualizaciones** > **Programa**.
2. Haga clic en **Activar actualizaciones programadas** y seleccione el programa de actualización.



3. Seleccione uno de los siguientes métodos de actualización:

    - **Sólo descargar**: seleccione esta casilla de verificación para descargar archivos del programa sin instalarlos. Aparecerá un mensaje en la consola del producto Web cuando las actualizaciones de archivos del programa estén listas para instalarse.

    - **Actualizar automáticamente después de descargar**: seleccione esta casilla de verificación para instalar automáticamente las actualizaciones de archivos del programa una vez que se hayan descargado.

        - **No actualizar automáticamente los programas que requieren reiniciar**: seleccione esta casilla de verificación para recibir un aviso en la consola del producto Web cuando la actualización requiera reiniciar. Las actualizaciones del programa que no requieran reiniciar se instalarán automáticamente.

4. Haga clic en **Guardar**.

Realizar actualizaciones manuales

Procedimiento

1. Vaya a **Actualizaciones** > **Programa**.

2. Seleccione uno de los siguientes métodos de actualización:

    - **Sólo descargar**: seleccione esta casilla de verificación para descargar archivos del programa sin instalarlos. Aparecerá un mensaje en la consola del producto Web cuando las actualizaciones de archivos del programa estén listas para instalarse.

    - **Actualizar automáticamente después de descargar**: seleccione esta casilla de verificación para instalar automáticamente las actualizaciones de archivos del programa una vez que se hayan descargado.

        - **No actualizar automáticamente los programas que requieren reiniciar**: seleccione esta casilla de verificación para recibir un aviso en la consola del producto Web cuando la actualización requiera reiniciar. Las

actualizaciones del programa que no requieran reiniciar se instalarán automáticamente.

3. Haga clic en **Guardar y actualizar ahora**.

Cargar archivos para realizar actualizaciones manuales

Procedimiento

1. Vaya a **Actualizaciones** > **Programa**.

Importante

Antes de continuar, asegúrese de que el Smart Protection Server no está llevando a cabo ninguna actualización. Si debe actualizar el programa o un componente, desactive primero las actualizaciones programadas de los componentes antes de continuar.

2. En **Cargar componente**, haga clic en **Examinar...** para localizar el archivo de programa para las actualizaciones manuales de los programas.

Nota

Localice el archivo del programa que ha descargado del sitio Web de Trend Micro o que Trend Micro le ha facilitado.

3. Localice el archivo y haga clic en **Abrir**.
4. Haga clic en **Cargar**.

Nota

Si ha desactivado la exploración programada para actualizar el programa o un componente, vuelva a activarla una vez que la descarga y la actualización hayan terminado.

Configurar una fuente de actualización

Utilice esta pantalla para especificar la fuente de actualización de File Reputation y de Reputación Web El origen de actualización predeterminado es el Trend Micro ActiveUpdate Server. Estas son las opciones disponibles en esta pantalla.

- **Trend Micro ActiveUpdate Server**: seleccione esta opción para descargar las actualizaciones de Trend Micro ActiveUpdate Server.
- **Otra fuente de actualización**: seleccione esta opción para especificar una fuente de actualización, como Trend Micro Control Manager.

Procedimiento

1. Vaya a **Actualizaciones** > **Origen** y seleccione la ficha **File Reputation** o **Reputación Web**.
2. Seleccione **Trend Micro ActiveUpdate Server** u **Otra fuente de actualización** y escriba una URL.
3. Haga clic en **Guardar**.

Tareas administrativas

Las tareas administrativas le permiten establecer la configuración del servicio SNMP, las notificaciones, la configuración del servidor proxy o descargar la información de diagnóstico.

Servicio SNMP

Smart Protection Server admite SNMP, que aporta flexibilidad para la supervisión del producto. Defina la configuración y descargue el archivo de la base de información de administración (MIB) de la pantalla **Servicio SNMP**. Estas son las opciones disponibles en esta pantalla.

- **Activar el servicio SNMP**: seleccione esta opción para utilizar SNMP.

- **Nombre de la comunidad**: especifique un nombre de la comunidad SNMP.
- **Activar la restricción de IP**: seleccione esta opción para activar la restricción de dirección IP.

Nota

El Encaminamiento inter-dominios sin clase (CIDR) no es compatible con la restricción de IP. Evite el acceso no autorizado al servicio SNMP mediante la activación de la restricción de dirección IP.

- **Dirección IP**: especifique una dirección IP para utilizar el servicio SNMP de supervisión del estado.
- **Máscara de subred**: especifique una máscara de red para determinar el rango de dirección IP para utilizar el servicio SNMP de supervisión del estado del equipo.
- **MIB del Servidor de Protección Inteligente**: haga clic en esta opción para descargar el archivo MIB del Servidor de Protección Inteligente.
- **Guardar**: haga clic en esta opción para conservar la configuración.
- **Cancelar**: haga clic en esta opción para desechar los cambios.

Configurar el servicio SNMP

Configure las opciones del servicio SNMP para que SNMP administre los sistemas y supervise el estado del Servidor de Protección Inteligente.

Procedimiento

1. Vaya a **Administración** > **Servicio SNMP**.

2. Seleccione la casilla de verificación **Activar el servicio SNMP**.
3. Especifique un **Nombre de la comunidad**.
4. Seleccione la casilla de verificación **Activar la restricción de IP** para evitar el acceso no autorizado al servicio SNMP.

> **Nota**
>
> El Encaminamiento inter-dominios sin clase (CIDR) no es compatible con la restricción de IP.

5. Especifique una dirección IP.
6. Especifique una máscara de subred.
7. Haga clic en **Guardar**.

Descargar el archivo MIB

Descargue el archivo MIB de la consola Web para utilizar el servicio SNMP.

Procedimiento

1. Vaya a **Administración** > **Servicio SNMP**.
2. Haga clic en **MIB del Servidor de Protección Inteligente** para descargar el archivo MIB. Aparecerá una ventana de confirmación.

3. Haga clic en **Guardar**.

   Aparecerá la pantalla **Guardar como**.

4. Especifique una ubicación en la que guardar el archivo.

5. Haga clic en **Guardar**.

MIB de Smart Protection Server

En la siguiente tabla se proporciona una descripción del archivo MIB del Servidor de Protección Inteligente.

Nombre del objeto	Identificador del objeto (OID)	Descripción
Trend-MIB:: Versión TBL	1.3.6.1.4.1.6101.1.2.1.1	Devuelve la versión actual de Smart Scan Pattern.
Trend-MIB:: TBLLastSuccessfulUpdate	1.3.6.1.4.1.6101.1.2.1.2	Devuelve la fecha y la hora de la última actualización de Smart Scan Pattern realizada con éxito.
Trend-MIB:: LastUpdateError	1.3.6.1.4.1.6101.1.2.1.3	Devuelve el estado de la última actualización de Smart Scan Pattern. • 0: la última actualización del patrón se realizó con éxito. • <código de error>: la última actualización del patrón no se realizó con éxito.
Trend-MIB:: LastUpdateErrorMessage	1.3.6.1.4.1.6101.1.2.1.4	Devuelve un mensaje de error si la última actualización de Smart Scan Pattern no se ha realizado correctamente.

Nombre del objeto	Identificador del objeto (OID)	Descripción
Trend-MIB:: WCSVersion	1.3.6.1.4.1.6101.1.2.1.5	Devuelve la versión actual de la Lista de bloqueo Web.
Trend-MIB:: WCSLastSuccessfulUpdate	1.3.6.1.4.1.6101.1.2.1.6	Devuelve la fecha y la hora de la última actualización de la Lista de bloqueo Web realizada con éxito.
Trend-MIB:: WCSLastUpdateError	1.3.6.1.4.1.6101.1.2.1.7	Devuelve el estado de la última actualización de la Lista de bloqueo Web. • 0: la última actualización del patrón se realizó con éxito. • <código de error>: la última actualización del patrón no se realizó con éxito.
Trend-MIB:: WCSLastUpdateErrorMessage	1.3.6.1.4.1.6101.1.2.1.8	Devuelve un mensaje de error si la última actualización de la Lista de Bloqueo Web no se ha realizado correctamente.
Trend-MIB:: LastVerifyError	1.3.6.1.4.1.6101.1.2.2.2	Devuelve el estado de la consulta de la File Reputation. • 0: la consulta de File Reputation tiene el comportamiento esperado. • <código de error>: la consulta de File Reputation no tiene el comportamiento esperado.

Nombre del objeto	Identificador del objeto (OID)	Descripción
Trend-MIB:: WCSLastVerifyError	1.3.6.1.4.1.6101.1.2.2.3	Devuelve el estado de la consulta de reputación Web. • 0: la consulta de Reputación Web tiene el comportamiento esperado. • <código de error>: la consulta de Reputación Web no tiene el comportamiento esperado.
Trend-MIB:: LastVerifyErrorMessage	1.3.6.1.4.1.6101.1.2.2.4	Devuelve un mensaje de error si el último estado de la consulta de la File Reputation no tuvo éxito.
Trend-MIB:: WCSLastVerifyErrorMessage	1.3.6.1.4.1.6101.1.2.2.5	Devuelve un mensaje de error si el último estado de la consulta de reputación Web no tuvo éxito.

MIB admitido

En la siguiente tabla se proporciona una descripción de otros MIB admitidos.

Nombre del objeto	Identificador del objeto (OID)	Descripción
SNMP MIB-2 System	1.3.6.1.2.1.1	El grupo del sistema incluye información acerca del sistema en el que reside la entidad. Los objetos de este grupo son útiles para la administración de errores y de la configuración. Consulte IETF RFC 1213.

Nombre del objeto	Identificador del objeto (OID)	Descripción
SNMP MIB-2 Interfaces	1.3.6.1.2.1.2	El grupo de objetos de interfaces contiene información acerca de cada interfaz de un dispositivo de red. Este grupo proporciona información útil acerca de la administración de errores, de la configuración, del rendimiento y de las cuentas. Consulte IETF RFC 2863.

Configuración del proxy

Si utiliza en la red un servidor proxy, configure los parámetros del proxy. Estas son las opciones disponibles en esta pantalla.

- **Usar un servidor proxy**: seleccione esta opción si su red utiliza un servidor proxy.
- **HTTP**: seleccione esta opción si su servidor proxy utiliza HTTP como protocolo de proxy.
- **SOCKS5**: seleccione esta opción si su servidor proxy utiliza SOCKS5 como protocolo de proxy.
- **Nombre del servidor o dirección IP**: escriba el nombre del servidor proxy o una dirección IP.
- **Puerto**: escriba el número de puerto.
- **ID de usuario**: escriba el ID de usuario del servidor proxy si su servidor proxy requiere autenticación.
- **Contraseña**: escriba la contraseña del servidor proxy si su servidor proxy requiere autenticación.

Configurar el proxy

Procedimiento

1. Vaya a **Administración** > **Configuración del proxy**.

2. Seleccione la casilla de verificación **Usar un servidor proxy** para las actualizaciones.

3. Seleccione los protocolos **HTTP** o **SOCKS5** para el proxy.

> **Nota**
>
> Smart Protection Server ya no es compatible con las configuraciones del proxy SOCKS4.

4. Escriba el nombre del servidor o una dirección IP.

5. escriba el número de puerto.

6. Si su servidor proxy requiere credenciales, escriba el **ID de usuario** y la **contraseña**.

7. Haga clic en **Guardar**.

Asistencia

Utilice la consola Web para descargar información de diagnóstico de solución de problemas y soporte.

Haga clic en **Inicio** para empezar a recopilar la información de diagnóstico.

Descargar información del sistema para el soporte

Procedimiento

1. Vaya a **Administración** > **Asistencia**.
2. Haga clic en **Iniciar**.

   Aparecerá la pantalla de progreso de la descarga.
3. Haga clic en **Guardar** cuando aparezca el mensaje de archivo descargado.
4. Especifique la ubicación y el nombre del archivo.
5. Haga clic en **Guardar**.

Cambiar la contraseña de la consola de producto

La contraseña de la consola de productos es el medio principal para proteger el Servidor de Protección Inteligente frente a cambios no autorizados. Para tener un entorno más seguro, cambie la contraseña de la consola regularmente y utilice una contraseña que sea difícil de adivinar. La contraseña de la cuenta de administrador se puede cambiar desde la interfaz de línea de comandos (CLI). Utilice el comando "configure password" de la CLI para realizar cambios.

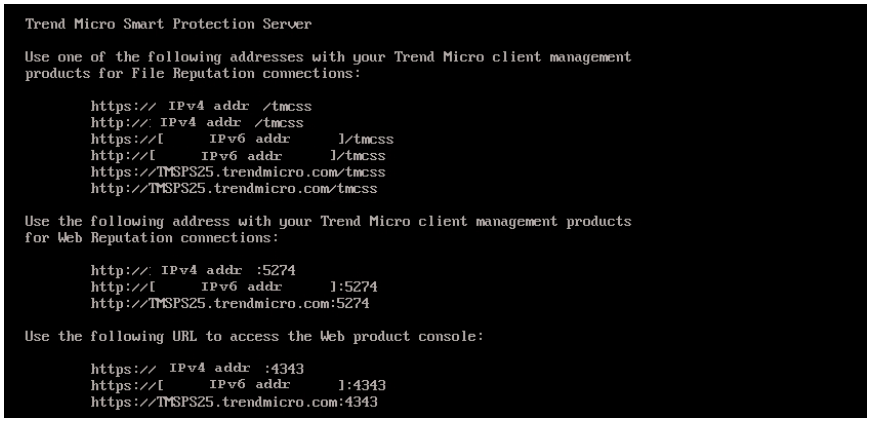
Consejo

Para elegir una contraseña segura, tenga en cuenta lo siguiente:

- Incluya tanto letras como números.
- Evite utilizar palabras que se encuentren en el diccionario (de cualquier idioma).
- Utilice palabras mal escritas de forma intencionada.
- Utilice frases o combine palabras.
- Utilice una combinación de mayúsculas y minúsculas.
- Utilice símbolos.

Procedimiento

1. Inicie sesión en la consola CLI con la cuenta de administrador.


Trend Micro Smart Protection Server
Use one of the following addresses with your Trend Micro client management products for File Reputation connections:
https:// IPv4 addr /tmcss
http:// IPv4 addr /tmcss
https://[IPv6 addr]/tmcss
http://[IPv6 addr]/tmcss
https://TMSPS25.trendmicro.com/tmcss
http://TMSPS25.trendmicro.com/tmcss
Use the following address with your Trend Micro client management products for Web Reputation connections:
http:// IPv4 addr :5274
http://[IPv6 addr]:5274
http://TMSPS25.trendmicro.com:5274
Use the following URL to access the Web product console:
https:// IPv4 addr :4343
https://[IPv6 addr]:4343
https://TMSPS25.trendmicro.com:4343

2. Escriba lo siguiente para activar los comandos de administración:

   `enable`

3. Escriba el siguiente comando:

   `configure password admin`

4. Escriba la nueva contraseña.

5. Escriba la nueva contraseña otra vez para confirmarla.

Capítulo 3

Supervisión de Smart Protection Server™

Supervise Trend Micro™ Smart Protection Server™ con registros y, desde la pantalla Resumen, mediante componentes.

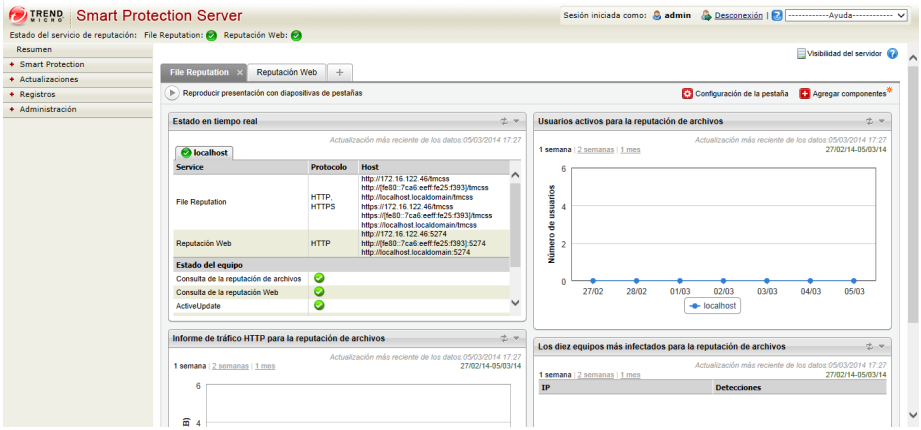
Los temas que se incluyen son:

- *Uso de la pantalla Resumen en la página 3-2*
- *Registros en la página 3-14*
- *Notificaciones en la página 3-18*

Uso de la pantalla Resumen

La pantalla **Resumen** puede mostrar información personalizada acerca de los servidores de Smart Protection Server, del tráfico y de las detecciones.

Smart Protection Server admite tanto el protocolo HTTP como HTTPS para las conexiones del Servicio de File Reputation y el protocolo HTTP para las conexiones del Servicio de Reputación Web. HTTPS proporciona una conexión más segura y HTTP utiliza menos ancho de banda. Las direcciones de los Servidores de Protección Inteligente aparecen en el banner de la consola de la interfaz de línea de comandos (CLI).



La pantalla **Resumen** consta de los siguientes elementos de la interfaz de usuario:

- **Visibilidad del servidor**: haga clic para agregar servidores a la lista Visibilidad del servidor o configurar los parámetros del servidor proxy para que se conecte a los servidores de la lista Visibilidad del servidor. La información de servidor se edita de igual forma en todos los componentes.

Nota

Las direcciones de los Servidores de Protección Inteligente se utilizan con los productos de Trend Micro para administrar puntos finales. Las direcciones de servidor se utilizan para configurar las conexiones de los puntos finales con los Servidores de Protección Inteligente.

- Las pestañas constituyen un área para los componentes. Para conocer más detalles, consulte *Pestañas en la página 3-3*.
- Los componentes son el elemento principal del panel. Para conocer más detalles, consulte *Componentes en la página 3-6*.

Pestañas

Las pestañas constituyen un área para los componentes. Cada pestaña de la pantalla **Resumen** puede contener hasta 20 componentes, y la pantalla **Resumen** admite hasta 30 pestañas.

Tareas de pestañas

En la siguiente tabla se muestran todas las tareas relacionadas con pestañas.

TAREA	PASOS
Agregar una pestaña	Haga clic en el icono más (+) en la parte superior de la pantalla **Resumen**. Se muestra la ventana **Nueva pestaña**. Si desea obtener información detallada sobre esta ventana, consulte *Ventana Nueva pestaña en la página 3-4*.
Editar la configuración de las pestañas	Haga clic en **Configuración de pestañas**. Se abre una ventana parecida a la ventana **Nueva pestaña**, donde puede editar la configuración.

TAREA	PASOS
Reproducir presentación con diapositivas de pestañas	Haga clic en **Reproducir presentación con diapositivas de pestañas**. La información de las pestañas seleccionadas cambia de forma parecida a una presentación con diapositivas.
Mover una pestaña	Arrastre y suelte la pestaña para cambiarla de posición.
Eliminar una pestaña	Haga clic en el icono de eliminación ( ) situado junto al título de la pestaña. Al eliminar una pestaña se eliminan también todos los componentes contenidos en ella.

Ventana Nueva pestaña

La ventana **Nueva pestaña** se abre cuando se agrega una nueva pestaña a la pantalla **Resumen**.

Esta ventana incluye las siguientes opciones:

Opción	Pasos
Cargo	Escriba el nombre de la pestaña.
Diseño	Elija uno de los diseños disponibles.
Presentación con diapositivas	La información de las pestañas seleccionadas cambia de forma parecida a una presentación con diapositivas. Si activa esta opción, puede seleccionar las pestañas que desea que aparezcan en la presentación, y también puede controlar la velocidad de la presentación.

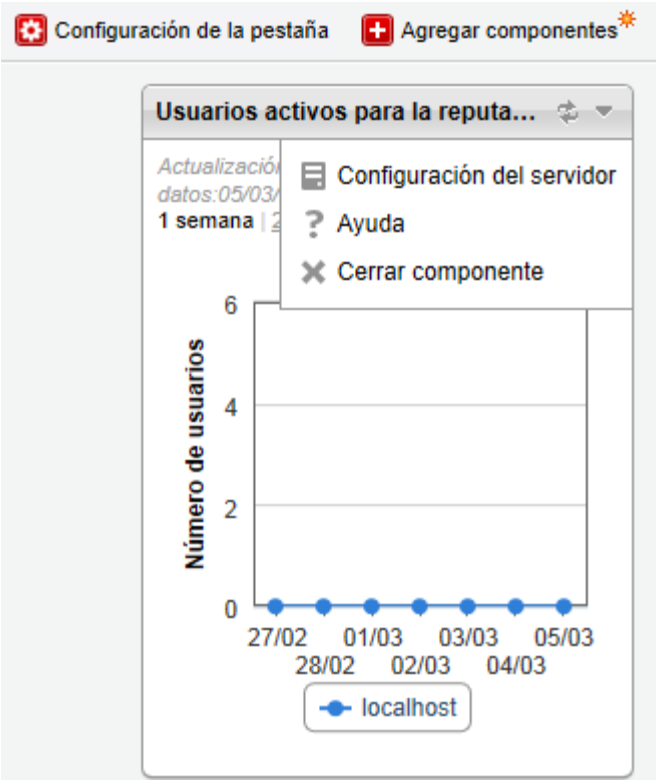
OPCIÓN	PASOS
Ajuste automático	El ajuste automático adapta el tamaño del componente al tamaño del cuadro.

Componentes

Los componentes le permiten personalizar la información que aparece en la pantalla **Resumen**. Se pueden agregar componentes nuevos a la consola Web. Puede arrastrar y soltar los componentes para personalizar el orden en el que aparecen. Los paquetes de componentes disponibles se pueden descargar y actualizar mediante la pantalla Actualización del programa. Después de actualizar el paquete de componentes, se puede agregar el componente nuevo desde la pantalla **Resumen**.

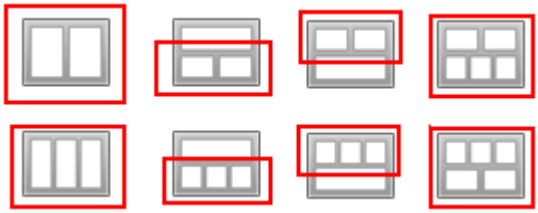
Tareas de componentes

En la siguiente tabla se muestran las tareas relacionadas con los componentes:



Tarea	Pasos
Agregar un componente	Abra una pestaña y, a continuación, haga clic en **Agregar componentes** en la esquina superior derecha. Aparecerá la pantalla **Agregar componentes**.
Actualizar los datos de los componentes	Haga clic en el icono de actualización ( ).

TAREA	PASOS
Definir la configuración del servidor	Haga clic en el icono de triángulo ( ) y, a continuación, haga clic en **Configuración del servidor** ( ) para incluir o excluir el componente en la recepción de información del servidor. También puede hacer clic en **Comprobar la visibilidad del servidor** para agregar servidores de la lista de visibilidad del servidor o configurar el proxy para establecer comunicación con los servidores de esta lista.
Ver ayuda	Haga clic en el icono de triángulo ( ) y, a continuación, haga clic en **Ayuda** ( ).
Eliminar un componente	Haga clic en el icono de triángulo ( ) y, a continuación, haga clic en **Cerrar componente** ( ). Esta acción elimina el componente de la pestaña que lo contiene, pero no de las otras pestañas que lo contienen ni de la lista de componentes de la pantalla **Agregar componentes**.
Mover un componente	Arrastre y suelte un componente para moverlo a otra ubicación dentro de la pestaña.

TAREA	PASOS
Cambiar el tamaño de un componente	Para cambiar el tamaño de un componente, sitúe el cursor en el borde derecho del componente. Cuando aparezca una línea vertical gruesa y una flecha (como muestra la siguiente imagen), mantenga pulsado y, a continuación, mueva el cursor a la izquierda o a la derecha. Solo los componentes de las pestañas que contienen varias columnas se pueden cambiar de tamaño. Estas pestañas tienen uno de los diseños siguientes y las secciones resaltadas contienen componentes cuyo tamaño se puede cambiar. 

Componentes disponibles

Los siguientes componentes se encuentran disponibles en esta versión.

Estado en tiempo real

Utilice el componente de estado en tiempo real para supervisar el estado de Smart Protection Server.

Nota

Cuando este complemento se muestra en la pantalla Resumen, la sesión de la consola del producto no caduca. El estado del equipo se actualiza cada minuto, lo que significa que la sesión no caduca debido a las consultas que se le envían al servidor. No obstante, la sesión caducará si la pestaña que se muestra actualmente no contiene este complemento.

TABLA 3-1. Datos del complemento

DATOS	DESCRIPCIÓN
Servicio	Servicios que proporciona Smart Protection Server.
Protocolo	Muestra los protocolos que admiten estos servicios. La File Reputation admite tanto el protocolo HTTP como el HTTPS. La Reputación Web admite el protocolo HTTP. HTTPS proporciona una conexión más segura y HTTP utiliza menos ancho de banda.
Host	Direcciones de los servicios de File Reputation y Reputación Web. Las direcciones se utilizan con los productos de Trend Micro que son compatibles con los Servidores de Protección Inteligente. Las direcciones se utilizan para configurar las conexiones de los Servidores de Protección Inteligente.
Estado del equipo	En Estado se muestran los siguientes elementos: • **Consulta de File Reputation**: muestra si la File Reputation está funcionando correctamente. • **Consulta de Reputación Web**: muestra si la Reputación Web está funcionando correctamente. • **ActiveUpdate**: muestra si ActiveUpdate está funcionando correctamente. • **Carga media de la CPU**: muestra la carga media del equipo de hace 1, 5 y 15 minutos generada por el kernel. • **Memoria disponible**: muestra la memoria física disponible del equipo. • **Cambiar el uso del disco**: muestra el uso del disco swap. • **Espacio libre**: muestra el espacio en disco libre que el equipo tiene disponible.

Usuarios activos para la Reputación de ficheros

El complemento Usuarios activos muestra el número de usuarios que han hecho consultas de File Reputation al Servidor de Protección Inteligente. Cada uno de los equipos cliente se considera un usuario activo.

Nota

Este componente muestra información en un gráfico 2D y se actualiza cada hora. También puede hacer clic en el icono de actualización ( ) en cualquier momento para actualizar los datos.

TABLA 3-2. Datos del complemento

DATOS	DESCRIPCIÓN
Usuarios	El número de usuarios que han enviado consultas a los Servidores de Protección Inteligente.
Fecha y hora	La fecha de la consulta.

Informe de tráfico HTTP para la Reputación de ficheros

El complemento de informe del tráfico HTTP muestra la cantidad total de tráfico de red en kilobytes (KB) que se ha enviado al Servidor de Protección Inteligente desde las consultas de File Reputation generadas por los clientes. La información de este complemento se actualiza cada hora y los datos se muestran en un gráfico de tres dimensiones. También puede hacer clic en el icono de actualización ( ) en cualquier momento para actualizar los datos.

Nota

En el gráfico de tres dimensiones, haga clic con el botón derecho del ratón para que se muestren las opciones para restablecer el gráfico o para que aparezca en 2D, 3D, 100% y con el mejor ajuste de tamaño. Puede también hacer clic en el nombre del servidor para que aparezcan en el gráfico los valores correspondientes a cada día.

TABLA 3-3. Datos del complemento

DATOS	DESCRIPCIÓN
Tráfico (KB)	El tráfico de red que han generado las consultas.
Fecha y hora	La fecha de las consultas.

Los 10 equipos más bloqueados para File Reputation

Este complemento muestra las direcciones IP de los 10 equipos que se han clasificado como equipos infectados después de que el Servidor de Protección Inteligente recibiese un virus conocido en una consulta de File Reputation. En este complemento, la información se muestra en una tabla en la que se incluye la dirección IP del equipo y el número total de detecciones de cada uno de ellos. La información de este componente se actualiza cada hora. También puede hacer clic en el icono de actualización ( ) en cualquier momento para actualizar los datos.

Utilice este componente para realizar un seguimiento de los equipos con el mayor número de infecciones de la red.

Nota

Si activa más de un Servidor de Protección Inteligente en este complemento, éste último calculará el número de detecciones del servidor que se seleccione y mostrará en la lista los 10 equipos más infectados de los Servidores de Protección Inteligente seleccionados.

TABLA 3-4. Datos del complemento

DATOS	DESCRIPCIÓN
IP	La dirección IP del equipo.
Detecciones	El número de amenazas de seguridad que este equipo ha detectado.

Usuarios activos para la Reputación Web

El complemento Usuarios activos muestra el número de usuarios que han hecho consultas de Reputación Web al Servidor de Protección Inteligente. Cada uno de los equipos cliente se considera un usuario activo.

Nota

Este componente muestra información en un gráfico 2D y se actualiza cada 5 minutos. También puede hacer clic en el icono de actualización ( ) en cualquier momento para actualizar los datos.

TABLA 3-5. Datos del complemento

DATOS	DESCRIPCIÓN
Usuarios	El número de usuarios que han enviado consultas a los Servidores de Protección Inteligente.
Fecha y hora	La fecha de la consulta.

Informe de tráfico HTTP para la Reputación Web

El complemento de informe del tráfico HTTP muestra la cantidad total de tráfico de red en kilobytes (KB) que se ha enviado al Servidor de Protección Inteligente desde las consultas de Reputación Web generadas por los clientes. La información de este complemento se actualiza cada hora y los datos se muestran en un gráfico de tres dimensiones. También puede hacer clic en el icono de actualización ( ) en cualquier momento para actualizar los datos.

Nota

En el gráfico de tres dimensiones, haga clic con el botón derecho del ratón para que se muestren las opciones para restablecer el gráfico o para que aparezca en 2D, 3D, 100% y con el mejor ajuste de tamaño. Puede también hacer clic en el nombre del servidor para que aparezcan en el gráfico los valores correspondientes a cada día.

TABLA 3-6. Datos del complemento

DATOS	DESCRIPCIÓN
Tráfico (KB)	El tráfico de red que han generado las consultas.
Fecha y hora	La fecha de las consultas.

Los diez equipos más bloqueados para la Reputación Web

Este componente muestra las direcciones IP de los 10 equipos que se han clasificado como equipos bloqueados después de que Smart Protection Server recibiese una URL en una consulta de Reputación Web. En este complemento, la información se muestra en una tabla en la que se incluye la dirección IP y el número total de URL bloqueadas en cada equipo. La información de este componente se actualiza diariamente. También puede hacer clic en el icono de actualización ( ) en cualquier momento para actualizar los datos.

Utilice este componente para realizar el seguimiento de los equipos que acceden al mayor número de sitios bloqueados de la red.

Nota

Si activa más de un Servidor de Protección Inteligente en este complemento, éste último calculará el número de detecciones del servidor que se seleccione y mostrará en la lista los 10 equipos más bloqueados de los Servidores de Protección Inteligente seleccionados.

TABLA 3-7. Datos del complemento

DATOS	DESCRIPCIÓN
IP	La dirección IP del equipo.
Detecciones	El número de URL bloqueadas de este equipo.

Registros

Utilice los registros para supervisar el estado del Servidor de Protección Inteligente. Para ver la información de los registros, realice una consulta.

Registro de acceso Web bloqueado

La pantalla de Registro de acceso Web bloqueado muestra información de las consultas de Reputación Web que devuelven resultados correspondientes a elementos malintencionados. Estas son las opciones disponibles en esta pantalla.

- **Palabra clave**: especifique las palabras clave que se van a utilizar en la búsqueda de URL.
- **Intervalo de fechas**: Seleccione un intervalo de tiempo.
- **Mostrar registro**: utilice las siguientes opciones para filtrar la consulta del registro:
  - **Todos**: muestra los registros de todos los sitios bloqueados.
  - **Bloqueado**: muestra los registros de los sitios que se bloquearon porque coincidían con una entrada de la lista de direcciones URL bloqueadas que ha definido el usuario.
  - **C&C para análisis virtual**: muestra los registros de los sitios que se bloquearon porque coincidían con una dirección URL o una dirección IP de la Lista de C&C para análisis virtual.
  - **Bloqueo Web**: muestra los registros de los sitios que se bloquearon porque coincidían con una dirección URL o una dirección IP de la Lista de bloqueo Web o de la Lista de C&C de Inteligencia global.
- **Origen de lista de C&C**: muestra los registros de los sitios que se bloquearon porque estaban en la lista de Inteligencia global o de Virtual Analyzer.

Detalles de registro:

- **Fecha y hora**: la fecha y la hora del evento de URL bloqueado.
- **URL**: La URL que la Reputación Web ha bloqueado.
- **Filtro**: la lista que activa el bloqueo de la dirección IP o URL. Podría ser la lista de direcciones URL bloqueadas que el usuario define, la Lista de C&C para análisis virtual o la Lista de bloqueo Web de Trend Micro.
- **Origen de lista de C&C**: puede ser la lista de Inteligencia global o la lista de Virtual Analyzer.
- **GUID del cliente**: la GUID del equipo que ha intentado acceder a la URL bloqueada.
- **GUID del servidor**: la GUID del producto de Trend Micro que admite Servidores de Protección Inteligente.

- **IP del cliente**: la dirección IP del equipo que ha intentado acceder a la URL bloqueada.
- **Equipo**: el nombre del equipo que ha intentado acceder a la URL bloqueada.
- **Usuario**: escriba el nombre de usuario del punto final.
- **Dominio**: el nombre del dominio del punto final.
- **Entidad del producto**: el producto de Trend Micro que ha detectado la URL.

Registro de actualización

La pantalla Registro de actualizaciones muestra información sobre las actualizaciones del archivo del programa o del patrón. Estas son las opciones disponibles en esta pantalla.

- **Intervalo de fechas**: seleccione el intervalo de fechas en el que se realizó la actualización.
- **Tipo**: seleccione el tipo de actualización que quiere que se muestre.

Detalles de registro:

- **Fecha y hora**: la fecha y la hora en que se actualizó el servidor.
- **Nombre del componente**: el componente que se actualizó.
- **Resultado**: puede ser correcto o incorrecto.
- **Descripción**: descripción del suceso de actualización.
- **Método de actualización**: indica si es exploración convencional o Smart Scan.

Registro de servicios de reputación

La ventana de Registro de servicios de reputación muestra información del estado de los servicios de Reputación Web y File Reputation. Estas son las opciones disponibles en esta pantalla.

- **Servicio**: especifique el servicio.
- **Resultado**: especifique el tipo de resultado.

- **Intervalo de fechas**: Seleccione un intervalo de tiempo.

Detalles de registro:

- **Fecha y hora**: la fecha y la hora en que la reputación comprobó el estado del servicio para los Servicios de Reputación Web y de File Reputation.
- **Servicio**: puede ser Reputación Web o File Reputation.
- **Resultado**: puede ser correcto o incorrecto.
- **Descripción**: se describe el estado del servicio para Reputación Web o File Reputation.

Mantenimiento de los registros

Realice el mantenimiento de los registros para eliminar los registros que ya no se necesiten. Estas son las opciones disponibles en esta pantalla.

- **Registro de actualización del patrón**: seleccione esta opción para purgar las entradas del registro de actualización del patrón.
- **Registro de actualización del programa**: seleccione esta opción para purgar las entradas del registro de actualización.
- **Registro de acceso Web bloqueado**: seleccione esta opción para purgar las entradas de consultas URL.
- **Registro de servicios de reputación**: seleccione esta opción para purgar las entradas de eventos de servicios de reputación.
- **Eliminar todos los registros**: seleccione esta opción para eliminar todos los registros.
- **Purgar los registros que sean anteriores al siguiente número de días**: seleccione esta opción para purgar los registros antiguos.
- **Activar la purga programada:** seleccione esta opción para programar la purga automática.

Procedimiento

1. Vaya a **Registros** > **Mantenimiento de los registros**.
2. Seleccione los tipos de registros que deben purgarse.
3. Seleccione eliminar todos los registros o los registros anteriores a un número de días específico.
4. Seleccione un programa de purga o haga clic en **Purgar ahora**.
5. Haga clic en **Guardar**.

Notificaciones

Puede configurar Smart Protection Server para que envíe un mensaje de correo electrónico o notificaciones mediante captura SNMP (Simple Network Management Protocol) a las personas designadas cuando se produzca un cambio de estado de los servicios o las actualizaciones.

Notificaciones por correo electrónico

Configure las opciones de las notificaciones por correo electrónico para enviar a los administradores mensajes por correo electrónico cuando haya un cambio de estado en los servicios o actualizaciones disponibles. Estas son las opciones disponibles en esta pantalla.

- **Servidor SMTP**: escriba la dirección IP del servidor SMTP.
- **Número de puerto**: escriba el número de puerto del servidor SMTP.
- **De**: escriba una dirección de correo electrónico para el campo del remitente de las notificaciones por correo electrónico.
- **Servicios**: seleccione esta opción para enviar notificaciones de los cambios de estado en File Reputation, Reputación Web y Actualización del patrón.
- **Para**: escriba una dirección de correo electrónico, o varias direcciones de correo electrónico, a las que enviar notificaciones de este evento.

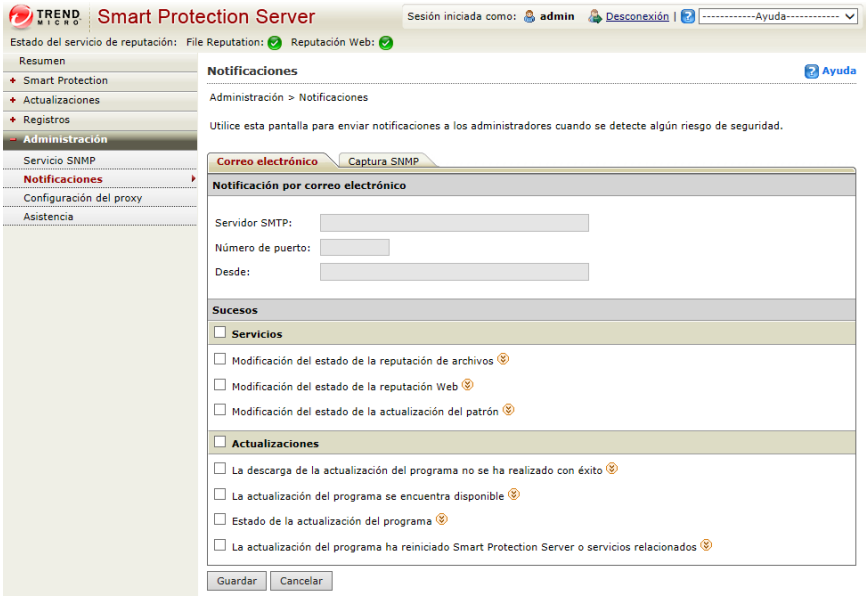
- **Asunto**: escriba un asunto nuevo o utilice el texto de asunto predeterminado para este evento.
- **Mensaje**: escriba un mensaje nuevo o utilice el texto de mensaje predeterminado para este evento.
- **Modificación del estado de la File Reputation**: seleccione esta opción para enviar una notificación con los cambios de estado y especifique el destinatario de esta notificación.
- **Modificación del estado de la reputación Web**: seleccione esta opción para enviar una notificación con los cambios de estado y especifique el destinatario de esta notificación.
- **Modificación del estado de la actualización del patrón**: seleccione esta opción para enviar una notificación con los cambios de estado y especifique el destinatario de esta notificación.
- **Actualizaciones**: seleccione esta opción para enviar notificaciones de todas las notificaciones relacionadas con el programa.
- **La descarga de la actualización del programa no se ha realizado con éxito**: seleccione esta opción para enviar una notificación si la actualización del programa no se ha descargado con éxito y especifique el destinatario de esta notificación.
- **La actualización del programa se encuentra disponible**: seleccione esta opción para enviar una notificación si la actualización del programa está disponible y hay que confirmarla, y especifique el destinatario de esta notificación.
- **Estado de la actualización del programa**: seleccione esta opción para enviar una notificación de que el programa se ha actualizado y especifique el destinatario de esta notificación.
- **La actualización del programa ha reiniciado el Servidor de Protección Inteligente o los servicios relacionados**: seleccione esta opción para enviar una notificación si el proceso de actualización del programa ha reiniciado el Servidor de Protección Inteligente o los servicios relacionados y especifique el destinatario de esta notificación.
- **Mensaje predeterminado**: haga clic en esta opción para que en los campos Asunto y Mensaje aparezca el texto predeterminado de Trend Micro.

Configurar notificaciones por correo electrónico

Procedimiento

1. Vaya a **Administración** > **Notificaciones** y, a continuación, vaya a la pestaña **Correo electrónico**.

   Aparecerá la pestaña Notificaciones por correo electrónico.



2. Seleccione la casilla de verificación **Servicios** para recibir una notificación por correo electrónico de los cambios de estado de todos los servicios o seleccione servicios concretos de las opciones que se muestran:

   - **Modificación del estado de la File Reputation**: seleccione esta opción para enviar una notificación con los cambios de estado y especifique el destinatario, el asunto y el mensaje.

- **Modificación del estado de la reputación Web**: seleccione esta opción para enviar una notificación con los cambios de estado y especifique el destinatario, el asunto y el mensaje.
- **Modificación del estado de la actualización del patrón**: seleccione esta opción para enviar una notificación con los cambios de estado y especifique el destinatario, el asunto y el mensaje.

3. Seleccione la casilla de verificación **Actualizaciones** o elija entre las siguientes opciones:
   - **La descarga de la actualización del programa no se ha realizado con éxito**: seleccione esta opción para enviar una notificación de este evento y especifique el destinatario, el asunto y el mensaje.
   - **La actualización del programa se encuentra disponible**: seleccione esta opción para enviar una notificación de este evento y especifique el destinatario, el asunto y el mensaje.
   - **Estado de la actualización del programa**: seleccione esta opción para enviar una notificación de este evento y especifique el destinatario, el asunto y el mensaje.
   - **La actualización del programa ha reiniciado el Servidor de Protección Inteligente o los servicios relacionados**: seleccione esta opción para enviar una notificación de este evento y especifique el destinatario, el asunto y el mensaje.
4. Escriba la dirección IP del servidor SMTP en el campo **Servidor SMTP**.
5. Escriba el número de puerto SMTP.
6. Escriba una dirección de correo electrónico en el campo **De**. Todas las notificaciones por correo electrónico aparecerán con esta dirección en el campo De de los mensajes de correo electrónico.
7. Haga clic en **Guardar**.

Notificaciones mediante captura SNMP

Configure las opciones de las notificaciones por Protocolo Simple de Administración de Redes (SNMP) para notificar a los administradores mediante captura SNMP cuando

haya un cambio de estado en los servicios. Estas son las opciones disponibles en esta pantalla.

- **Dirección IP del servidor**: especifique la dirección IP del destinatario de la captura SNMP.
- **Nombre de la comunidad**: especifique el nombre de la comunidad SNMP.
- **Servicios**: seleccione esta opción para enviar una notificación SNMP en la que se informe de los cambios de estado de la File Reputation, la Reputación Web y las actualizaciones de patrones.
- **Mensaje**: escriba un mensaje nuevo o utilice el texto de mensaje predeterminado para este evento.
- **Modificación del estado de la File Reputation**: seleccione esta opción para enviar una notificación con los cambios de estado.
- **Modificación del estado de la reputación Web**: seleccione esta opción para enviar una notificación con los cambios de estado.
- **Modificación del estado de la actualización del patrón**: seleccione esta opción para enviar una notificación con los cambios de estado.
- **Mensaje predeterminado**: haga clic en esta opción para que en los campos Mensaje aparezca el texto predeterminado de Trend Micro.

Configurar las notificaciones mediante captura SNMP

Configure las opciones de las notificaciones por Protocolo Simple de Administración de Redes (SNMP) para notificar a los administradores mediante captura SNMP cuando haya un cambio de estado en los servicios.

Procedimiento

1. Vaya a **Administración** > **Notificaciones** y, a continuación, vaya a la pestaña **SNMP**.

Aparecerá la pestaña Notificaciones mediante captura SNMP.

2. Seleccione la casilla de verificación **Servicios** o las siguientes casillas de verificación:

   - **Modificación del estado de la File Reputation**: seleccione esta opción para enviar una notificación con los cambios de estado y especifique el destinatario, el asunto y el mensaje.
   - **Modificación del estado de la reputación Web**: seleccione esta opción para enviar una notificación con los cambios de estado y especifique el destinatario, el asunto y el mensaje.
   - **Modificación del estado de la actualización del patrón**: seleccione esta opción para enviar una notificación con los cambios de estado y especifique el destinatario, el asunto y el mensaje.

3. Escriba la dirección IP del servidor de captura SNMP.

4. Escriba el nombre de la comunidad SNMP.

5. Haga clic en **Guardar**.

Capítulo 4

Obtener ayuda

En este capítulo incluye información detallada acerca de cómo obtener ayuda adicional mientras se trabaja con Trend Micro™ Smart Protection Server™.

Los temas que se incluyen son:

- *Uso del portal de asistencia en la página 4-2*
- *Enciclopedia de amenazas en la página 4-3*
- *Ponerse en contacto con Trend Micro en la página 4-4*
- *TrendLabs en la página 4-5*

Uso del portal de asistencia

El portal de Trend Micro Support es un recurso en línea disponible las 24 horas del día, 7 días a la semana que contiene la información más actualizada acerca de problemas comunes y otros menos habituales.

Procedimiento

1. Vaya a http://esupport.trendmicro.com.
2. Seleccione un producto o servicio de la lista desplegable adecuada y especifique otra información relacionada.

   Se muestra la página del producto de **Asistencia técnica**.
3. Utilice el cuadro **Buscar asistencia** para buscar las soluciones disponibles.
4. Si no se encuentra ninguna solución, haga clic en **Enviar un caso de asistencia** en el panel de navegación izquierdo y agregue los detalles pertinentes o envíe un caso de asistencia aquí:

   http://esupport.trendmicro.com/srf/SRFMain.aspx

   Un ingeniero de asistencia de Trend Micro investigará el caso y responderá en 24 horas o menos.

Problemas conocidos

En los problemas conocidos se documenta el comportamiento inesperado del producto para el que puede ser necesario realizar tareas adicionales temporales. Trend Micro recomienda que compruebe siempre el archivo Léame para obtener información sobre los requisitos del sistema y los problemas conocidos que pueden afectar a la instalación o al rendimiento. Los archivos Léame también contienen una descripción de las novedades de cada versión en particular y otra información de utilidad.

Los problemas conocidos más recientes y sus posibles soluciones también se pueden encontrar en la base de conocimientos de Trend Micro:

http://esupport.trendmicro.com

Archivos hotfix, parches y service packs

Tras el lanzamiento oficial de un producto, Trend Micro suele desarrollar archivos Hotfix de corrección, parches y service packs para solucionar algunos problemas pendientes, mejorar el rendimiento del producto e incluir nuevas funciones.

A continuación encontrará un resumen de los componentes que puede publicar Trend Micro:

- **Archivo hotfix**: una solución a los problemas notificados por los clientes. Trend Micro desarrolla y publica archivos Hotfix solo para clientes específicos.
- **Revisión de seguridad**: un solo archivo hotfix o un grupo de ellos adecuado para implementarlos en todos los clientes.
- **Revisión**: un grupo de revisiones de seguridad adecuado para implementarlo en todos los clientes.
- **Service Pack**: una mejora significativa de las funciones que actualizan el producto.

El distribuidor o proveedor de asistencia puede ponerse en contacto con el usuario cuando estos elementos están disponibles. Visite el sitio Web de Trend Micro para obtener más información sobre las nuevas publicaciones de archivos Hotfix, revisiones y service packs:

http://downloadcenter.trendmicro.com/?regs=ES

Todas las publicaciones incluyen un archivo Léame que contiene información sobre la instalación, implementación y configuración. Lea detenidamente el archivo Léame antes de efectuar la instalación.

Enciclopedia de amenazas

La mayoría del malware de hoy en día consta de "amenazas mezcladas", es decir, una o varias tecnologías combinadas mediante protocolos de seguridad informática de omisión. Trend Micro combate este malware complejo con productos que crean una

estrategia de defensa personalizada. La Enciclopedia de amenazas ofrece una lista completa de nombres y síntomas de diversas amenazas mezcladas, lo que incluye malware conocido, spam, URL maliciosas y vulnerabilidades conocidas.

Vaya a http://www.trendmicro.com/vinfo/es/virusencyclo/default.asp para obtener más información acerca de:

- Malware o código móvil malicioso actualmente en circulación
- Páginas de información correlacionada sobre amenazas para crear una historia completa de ataques Web
- Advertencias sobre amenazas Web relacionadas con ataques dirigidos y amenazas de seguridad
- Ataques Web e información en línea sobre tendencias
- Informes semanales sobre malware.

Ponerse en contacto con Trend Micro

Puede ponerse en contacto con los agentes de Trend Micro por teléfono, fax, o correo electrónico:

Dirección	TREND MICRO INCORPORATED TREND MICRO España Plaza de las Cortes, 4 – 8º Izq. Madrid, 28014 España
Teléfono	+34 91 369 70 30
Fax:	+34 91 369 70 31
Sitio Web	http://www.trendmicro.com
Dirección de correo electrónico	reception_es@trendmicro.es

- Oficinas de asistencia técnica de todo el mundo:

  http://www.trendmicro.es/acerca/contacto/index.html

- Documentación de productos de Trend Micro:

  http://docs.trendmicro.com/es-es/home.aspx

Agilizar la llamada al servicio de asistencia

Para mejorar la resolución de problemas, tenga a mano la siguiente información:

- Pasos para reproducir el problema
- Información del aparato o la red
- Marca y modelo del equipo informático, junto con el hardware adicional conectado al punto final
- Cantidad de memoria y espacio libre en el disco duro
- Sistema operativo y versión del Service Pack
- Versión del cliente del punto final
- Número de serie o código de activación
- Descripción detallada del entorno de instalación
- Texto exacto de cualquier mensaje de error recibido.
- Plataforma de virtualización (VMware™ o Hyper-V™) y versión

TrendLabs

TrendLabs℠ es una red global de centros de investigación, desarrollo y acción comprometida a la vigilancia de amenazas, la prevención frente a ataques y la entrega de soluciones completas y a tiempo, las 24 horas del día, los 7 días de la semana. TrendLabs funciona como columna vertebral de la infraestructura de servicios de Trend Micro; a tal efecto, se sirve de un equipo de varios cientos de ingenieros y personal de asistencia técnica certificado que ofrecen una amplia gama de servicios de asistencia tanto técnica como de productos.

TrendLabs supervisa el panorama mundial de amenazas para proporcionar medidas de seguridad efectivas diseñadas para detectar, prevenir y eliminar ataques. La culminación

diaria de estos esfuerzos se hace llegar a los clientes por medio de constantes actualizaciones de archivos de patrones de virus y mejoras del motor de exploración.

Puede encontrar más información sobre TrendLabs en:

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

Apéndice A

Comandos de la Interfaz de línea de comandos (CLI)

En esta sección se describen los comandos de la Interfaz de línea de comandos (CLI) que puede utilizar en el producto para llevar a cabo las tareas de supervisión, depuración, resolución de problemas y configuración. Inicie sesión en la CLI mediante la máquina virtual con la cuenta de administrador. Los comandos de la CLI permiten a los administradores realizar tareas de configuración y llevar a cabo funciones de depuración y resolución de problemas. La interfaz CLI también proporciona comandos adicionales para supervisar los recursos y funciones fundamentales. Para acceder a la interfaz CLI, tiene que tener la cuenta de administrador y la contraseña.

COMANDO	SINTAXIS	DESCRIPCIÓN
configure date	**configure date** <date> <time>	Configura la fecha y la guarda en el CMOS *fecha* DATE_FIELD [DATE_FIELD] *hora* TIME_FIELD [TIME_FIELD]

COMANDO	SINTAXIS	DESCRIPCIÓN
configure dns ipv4	**configurar dns ipv4** <dns1> [dns2]	Configura los ajustes de DNS IPv4 *dns1* IPv4_ADDR Servidor DNS primario *dns2* IPv4_ADDR Servidor DNS secundario []
configure dns ipv6	**configure dns ipv6** <dns1> [dns2]	Configura los ajustes de DNS IPv6. *dns1* IPv6_ADDR Servidor DNS primario *dns2* IPv6_ADDR Servidor DNS secunsario []
configure hostname	**configure hostname** <hostname>	Configura el nombre de host *hostname* HOSTNAME Nombre de host o FQDN
configure locale de_DE	**configure locale de_DE**	Configura el sistema local en alemán.
configure locale en_US	**configure locale en_US**	Configura el sistema local en inglés.
configure locale es_ES	**configure locale es_ES**	Configura el sistema local en español.
configure locale fr_FR	**configure locale fr_FR**	Configura el sistema local en francés.
configure locale it_IT	**configure locale it_IT**	Configura el sistema local en italiano.
configure locale ja_JP	**configure locale ja_JP**	Configura el sistema local en japonés.
configure locale ko_KR	**configure locale ko_KR**	Configura el sistema local en coreano.

Comando	Sintaxis	Descripción
configure locale ru_RU	**configure locale ru_RU**	Configura el sistema local en ruso.
configure locale zh_CN	**configure locale zh_CN**	Configura el sistema local en chino (simplificado).
configure locale zh_TW	**configure locale zh_TW**	Configura el sistema local en chino (tradicional).
configure ntp	**configure ntp <ip or FQDN>**	Configurar el servidor NTP
configure port	**configure port <frs_http_port> <frs_https_port> <wrs_http_port>**	Para cambiar los puertos de servicio de los Servicios de Reputación Web o de File Reputation
configure ipv4 dhcp	**configure ipv4 dhcp [vlan]**	Configura la interfaz Ethernet predeterminada para utilizar DHCP. *vlan* VLAN_ID VLan ID [1-4094], default none VLan: [0]
configure ipv4 static	**configure ipv4 static** <ip> <mask> <gateway> [vlan]	Configura la interfaz Ethernet predeterminada para utilizar la configuración IPv4 estática. *vlan* VLAN_ID VLan ID [1-4094], default none VLan: [0]
configure ipv6 auto	**configure ipv6 auto** [vlan]	Configura la interfaz Ethernet predeterminada para utilizar la configuración IPv6 de detección automática de vecinos. *vlan* VLAN_ID VLan ID [1-4094], default none VLan: [0]

COMANDO	SINTAXIS	DESCRIPCIÓN
configure ipv6 dhcp	**configure ipv6 dhcp** [vlan]	Configura la interfaz Ethernet predeterminada para utilizar la configuración IPv6 dinámica (DHCPv6). *vlan* VLAN_ID VLan ID [1-4094], default none VLan: [0]
configure ipv6 static	**configure ipv6 static** <v6ip> <v6mask> <v6gate> [vlan]	Configura la interfaz Ethernet predeterminada para utilizar la configuración IPv6 estática. *vlan* VLAN_ID VLan ID [1-4094], default none VLan: [0]
configure password	**configure password** <usuario>	Configurar la contraseña de la cuenta *user* USER El nombre de usuario cuya contraseña desea cambiar. El usuario puede ser "admin", "root" o cualquier usuario del grupo de administradores del servidor de Smart Protection Server.
configure service	**configure service interface** <ifname>	Establece la configuración de servidor predeterminada.
configure timezone Africa Cairo	**configure timezone Africa Cairo**	Configura la zona horaria como África/Cairo.
configure timezone Africa Harare	**configure timezone Africa Harare**	Configura la zona horaria como África/Harare.
configure timezone Africa Nairobi	**configure timezone Africa Nairobi**	Configura la zona horaria como África/Nairobi.

Comando	Sintaxis	Descripción
`configure timezone America Anchorage`	`configure timezone America Anchorage`	Configura la zona horaria para América/Anchorage.
`configure timezone America Bogota`	`configure timezone America Bogota`	Configura la zona horaria como América/Bogotá.
`configure timezone America Buenos_Aires`	`configure timezone America Buenos_Aires`	Configura la zona horaria para América/Buenos Aires.
`configure timezone America Caracas`	`configure timezone America Caracas`	Configura la zona horaria como América/Caracas.
`configure timezone America Chicago`	`configure timezone America Chicago`	Configura la zona horaria como América/Chicago.
`configure timezone America Chihuahua`	`configure timezone America Chihuahua`	Configura la zona horaria como América/Chihuahua.
`configure timezone America Denver`	`configure timezone America Denver`	Configura la zona horaria como América/Denver.
`configure timezone America Godthab`	`configure timezone America Godthab`	Configura la zona horaria como América/Godthab.
`configure timezone America Lima`	`configure timezone America Lima`	Configura la zona horaria como América/Lima.
`configure timezone America Los_Angeles`	`configure timezone America Los_Angeles`	Configura la zona horaria como América/Los Ángeles.
`configure timezone America Mexico_City`	`configure timezone America Mexico_City`	Configura la zona horaria como América/Ciudad de México.
`configure timezone America New_York`	`configure timezone America New_York`	Configura la zona horaria como América/Nueva York.
`configure timezone America Noronha`	`configure timezone America Noronha`	Configura la zona horaria como América/Noronha.
`configure timezone America Phoenix`	`configure timezone America Phoenix`	Configura la zona horaria como América/Phoenix.

COMANDO	SINTAXIS	DESCRIPCIÓN
`configure timezone America Santiago`	`configure timezone America Santiago`	Configura la zona horaria como América/Santiago.
`configure timezone America St_Johns`	`configure timezone America St_Johns`	Configura la zona horaria como América/St Johns.
`configure timezone America Tegucigalpa`	`configure timezone America Tegucigalpa`	Configura la zona horaria como América/Tegucigalpa.
`configure timezone Asia Almaty`	`configure timezone Asia Almaty`	Configura la zona horaria como Asia/Almaty.
`configure timezone Asia Baghdad`	`configure timezone Asia Baghdad`	Configura la zona horaria como Asia/Baghdad.
`configure timezone Asia Baku`	`configure timezone Asia Baku`	Configura la zona horaria como Asia/Baku.
`configure timezone Asia Bangkok`	`configure timezone Asia Bangkok`	Configura la zona horaria como Asia/Bangkok.
`configure timezone Asia Calcutta`	`configure timezone Asia Calcutta`	Configura la zona horaria como Asia/Calcuta.
`configure timezone Asia Colombo`	`configure timezone Asia Colombo`	Configura la zona horaria como Asia/Colombo.
`configure timezone Asia Dhaka`	`configure timezone Asia Dhaka`	Configura la zona horaria como Asia/Dhaka.
`configure timezone Asia Hong_Kong`	`configure timezone Asia Hong_Kong`	Configura la zona horaria como Asia/Hong Kong.
`configura la zona horaria como Asia/ Irkutsk`	`configura la zona horaria como Asia/Irkutsk`	Configura la zona horaria como Asia/Irkutsk.
`configure timezone Asia Jerusalem`	`configure timezone Asia Jerusalem`	Configura la zona horaria como Asia/Jerusalén.
`configure timezone Asia Kabul`	`configure timezone Asia Kabul`	Configura la zona horaria como Asia/Kabul.

Comando	Sintaxis	Descripción
`configure timezone Asia Karachi`	`configure timezone Asia Karachi`	Configura la zona horaria como Asia/Karachi.
`configure timezone Asia Katmandu`	`configure timezone Asia Katmandu`	Configura la zona horaria como Asia/Katmandú.
`configure timezone Asia Krasnoyarsk`	`configure timezone Asia Krasnoyarsk`	Configura la zona horaria como Asia/Krasnoyarsk.
`configure timezone Asia Kuala_Lumpur`	`configure timezone Asia Kuala_Lumpur`	Configura la zona horaria como Asia/Kuala.
`configure timezone Asia Kuwait`	`configure timezone Asia Kuwait`	Configura la zona horaria como Asia/Kuwait.
`configure timezone Asia Magadan`	`configure timezone Asia Magadan`	Configura la zona horaria como Asia/Magadán.
`configure timezone Asia Manila`	`configure timezone Asia Manila`	Configura la zona horaria como Asia/Manila.
`configure timezone Asia Muscat`	`configure timezone Asia Muscat`	Configura la zona horaria como Asia/Muscat.
`configure timezone Asia Rangoon`	`configure timezone Asia Rangoon`	Configura la zona horaria como Asia/Rangoon.
`configure timezone Asia Seoul`	`configure timezone Asia Seoul`	Configura la zona horaria como Asia/Seúl.
`configure timezone Asia Shanghai`	`configure timezone Asia Shanghai`	Configura la zona horaria como Asia/Shanghai.
`configure timezone Asia Singapore`	`configure timezone Asia Singapore`	Configura la zona horaria como Asia/Singapur.
`configure timezone Asia Taipei`	`configure timezone Asia Taipei`	Configura la zona horaria como Asia/Taipei.
`configure timezone Asia Tehran`	`configure timezone Asia Tehran`	Configura la zona horaria como Asia/Teherán.

COMANDO	SINTAXIS	DESCRIPCIÓN
`configura la zona horaria como Asia/Tokio`	`configura la zona horaria como Asia/Tokio`	Configura la zona horaria como Asia/Tokio.
`configure timezone Asia Yakutsk`	`configure timezone Asia Yakutsk`	Configura la zona horaria como Asia/Yakutsk.
`configure timezone Atlantic Azores`	`configure timezone Atlantic Azores`	Configura la zona horaria como Atlántico/Azores.
`configure timezone Australia Adelaide`	`configure timezone Australia Adelaide`	Configura la zona horaria como Australia/Adelaida.
`configure timezone Australia Brisbane`	`configure timezone Australia Brisbane`	Configura la zona horaria como Australia/Brisbane.
`configure timezone Australia Darwin`	`configure timezone Australia Darwin`	Configura la zona horaria como Australia/Darwin.
`configure timezone Australia Hobart`	`configure timezone Australia Hobart`	Configura la zona horaria como Australia/Hobart.
`configure timezone Australia Melbourne`	`configure timezone Australia Melbourne`	Configura la zona horaria como Australia/Melbourne.
`configure timezone Australia Perth`	`configure timezone Australia Perth`	Configura la zona horaria como Australia/Perth.
`configure timezone Europe Amsterdam`	`configure timezone Europe Amsterdam`	Configura la zona horaria como Europa/Ámsterdam
`configure timezone Europe Athens`	`configure timezone Europe Athens`	Configura la zona horaria como Europa/Atenas.
`configure timezone Europe Belgrade`	`configure timezone Europe Belgrade`	Configura la zona horaria como Europa/Belgrado.
`configure timezone Europe Berlin`	`configure timezone Europe Berlin`	Configura la zona horaria como Europa/Berlín.
`configure timezone Europe Brussels`	`configure timezone Europe Brussels`	Configura la zona horaria como Europa/Bruselas.

Comando	Sintaxis	Descripción
`configure timezone Europe Bucharest`	`configure timezone Europe Bucharest`	Configura la zona horaria como Europa/Bucarest.
`configura la zona horaria como Europa/Dublín`	`configura la zona horaria como Europa/Dublín`	Configura la zona horaria como Europa/Dublín.
`configure timezone Europe Moscow`	`configure timezone Europe Moscow`	Configura la zona horaria como Europa/Moscú.
`configure timezone Europe Paris`	`configure timezone Europe Paris`	Configura la zona horaria como Europa/París.
`configure timezone Pacific Auckland`	`configure timezone Pacific Auckland`	Configura la zona horaria como Pacífico/Auckland.
`configure timezone Pacific Fiji`	`configure timezone Pacific Fiji`	Configura la zona horaria como Pacífico/Fiji.
`configura la zona horaria como Pacífico/Guam`	`configura la zona horaria como Pacífico/Guam`	Configura la zona horaria como Pacífico/Guam.
`configure timezone Pacific Honolulu`	`configure timezone Pacific Honolulu`	Configura la zona horaria como Pacífico/Honolulu.
`configure timezone Pacific Kwajalein`	`configure timezone Pacific Kwajalein`	Configura la zona horaria como Pacífico/Kwajalein.
`configure timezone Pacific Midway`	`configure timezone Pacific Midway`	Configura la zona horaria como Pacífico/Midway.
`configure timezone US Alaska`	`configure timezone US Alaska`	Configura la zona horaria como EE. UU./Alaska.
`configura la zona horaria como EE. UU./Arizona`	`configura la zona horaria como EE. UU./Arizona`	Configura la zona horaria como EE. UU./Arizona.
`configure timezone US Central`	`configure timezone US Central`	Configura la zona horaria como EE. UU./Central.

COMANDO	SINTAXIS	DESCRIPCIÓN
`configure timezone US East-Indiana`	`configure timezone US East-Indiana`	Configura la zona horaria como EE. UU./East Indiana.
`configure timezone US Eastern`	`configure timezone US Eastern`	Configura la zona horaria como EE. UU./Este.
`configure timezone US Hawaii`	`configure timezone US Hawaii`	Configura la zona horaria como EE. UU./Hawaii.
`configure timezone US Mountain`	`configure timezone US Mountain`	Configura la zona horaria como EE. UU./Mountain.
`configure timezone US Pacific`	`configure timezone US Pacific`	Configura la zona horaria como EE. UU./Pacífico.
`disable adhoc-query`	`disable adhoc-query`	Desactiva el Registro de acceso Web.
`disable ssh`	`disable ssh`	Desactiva el demonio sshd.
`enable`	`enable`	Activa los comandos de administración.
`enable adhoc-query`	`enable adhoc-query`	Activa el Registro de acceso Web.
`enable hyperv-ic`	`enable hyperv-ic`	Activa los componentes de integración de Linux Hyper-V en el Servidor de Protección Inteligente.
`enable ssh`	`enable ssh`	Activa el demonio sshd.
`exit`	`exit`	Sale de la sesión.
`ayuda`	`ayuda`	Muestra información general de la sintaxis de la CLI.

Comando	Sintaxis	Descripción
history	**history** [limit]	Mostrar el historial de la línea de comandos de la sesión actual *limit*especifica el número de comandos de la CLI que se van a mostrar. Ejemplo: Especificar un valor de *límit* de «5» significa que se muestran 5 comandos CLI.
reboot	**reboot** [time]	Reiniciar el equipo después de un intervalo de tiempo especificado o de forma inmediata *time*UNIT Tiempo en minutos para reiniciar esta máquina [0].
show date	**show date**	Muestra la fecha y hora actuales.
show hostname	**show hostname**	Muestra el nombre de host de la red.
show interfaces	**show interfaces**	Muestra la información de las interfaces de red.
show ipv4 address	**show ipv4 address**	Muestra la dirección IPv4 de la red.
show ipv4 dns	**show ipv4 dns**	Muestra los servidores DNS IPv4 de la red.
show ipv4 gateway	**show ipv4 gateway**	Muestra el gateway IPv4 de la red.
show ipv4 route	**show ipv4 route**	Muestra la tabla de enrutamiento IPv4 de la red

COMANDO	SINTAXIS	DESCRIPCIÓN
`show ipv4 type`	`show ipv4 type`	Muestra el tipo de configuración IPv4 de la red (dhcp / estático).
`show ipv6 address`	`show ipv6 address`	Muestra la dirección IPv6 de la red.
`show ipv6 dns`	`show ipv6 dns`	Muestra los servidores DNS IPv6 de la red.
`show ipv6 gateway`	`show ipv6 gateway`	Muestra el gateway IPv6 de la red.
`show ipv6 route`	`show ipv6 route`	Muestra la tabla de enrutamiento IPv6 de la red.
`show ipv6 type`	`show ipv6 type`	Muestra el tipo de configuración IPv6 de la red (dhcp / estático).
`show timezone`	`show timezone`	Muestra la zona horaria de la red.
`show uptime`	`show uptime`	Muestra el tiempo de funcionamiento actual del sistema.
`show url management`	`show url management`	Muestra la URL de la consola de administración Web.
`show url FileReputationService`	`show url FileReputationService`	Muestra las direcciones de conexión del punto final para los Servicios de File Reputation
`show url WebReputationService`	`show url WebReputationService`	Muestra las direcciones de conexión del punto final para los Servicios de Reputación Web

Comando	Sintaxis	Descripción
shutdown	**shutdown** [time]	Apaga la máquina después de un intervalo de tiempo especificado o de forma inmediata. *time*UNIT Tiempo en minutos para apagar esta máquina [0].

Apéndice B

Glosario

En este glosario se describen los términos relacionados con el uso de Smart Protection Server.

TÉRMINO	DEFINICIÓN
activar	Habilita el software una vez completado el proceso de registro. Los productos de Trend Micro no funcionarán hasta que no se realice su activación. Actívelos durante la instalación o una vez instalados (en la consola de administración) desde la pantalla Licencia del producto.
ActiveUpdate	ActiveUpdate es una función incorporada en numerosos productos de Trend Micro. Conectada al sitio Web de actualizaciones de Trend Micro, ActiveUpdate ofrece descargas actualizadas de los archivos de patrones de virus, los motores de exploración y los archivos de programa, a través de Internet o del CD Total Solution de Trend Micro.
dirección	Hace referencia a una dirección de red (consulte dirección IP) o a una dirección de correo electrónico, que es la cadena de caracteres que especifican el origen o el destino de un mensaje de correo electrónico.
administrador	Se refiere al administrador del sistema, es decir, el responsable en una empresa de actividades como la instalación de nuevo hardware y software, la asignación de nombres de usuario y contraseñas, la supervisión del espacio en disco y otros recursos de TI, la realización de copias de seguridad y la administración de la seguridad de la red.

TÉRMINO	DEFINICIÓN
cuenta de administrador	Un nombre de usuario y una contraseña con derechos de administrador.
antivirus	Programas informáticos diseñados para detectar y eliminar virus.
autenticación	Verificación de la identidad de una persona o de un proceso. La autenticación garantiza que se realiza la transmisión de datos digitales al destinatario previsto. Asimismo, también garantiza al receptor la integridad del mensaje y la fuente de éste (su procedencia). La forma más simple de autenticación requiere un nombre de usuario y una contraseña para acceder a una cuenta determinada. Además, los protocolos de autenticación pueden estar basados en cifrados de clave secreta, como el algoritmo estándar de cifrado de datos (DES), o en sistemas de clave pública mediante firmas digitales. Consulte también cifrado de clave pública y firma digital.
cliente	Un sistema o proceso informático que solicita un servicio a otro sistema o proceso informático (un servidor) a través de un tipo de protocolo y que acepta las respuestas del servidor. Un cliente forma parte de la arquitectura informática de cliente-servidor.
configuración	Selecciona las opciones de funcionamiento del producto de Trend Micro como, por ejemplo, elegir si los mensajes de correo infectados con virus se podrán en cuarentena o se eliminarán.
Predeterminado	Un valor que se rellena automáticamente en un campo de la interfaz de la consola de administración. Un valor predeterminado representa una elección lógica y se suministra para un uso más cómodo del programa. Utilice valores predeterminados tal cual o cámbielos.
(administrativo) dominio	Grupo de equipos que comparten una base de datos y una política de seguridad común.
Nombre de dominio	El nombre completo de un sistema compuesto por el nombre del host local y su nombre de dominio (por ejemplo, tellsitall.com). Un nombre de dominio debe bastar para determinar una dirección exclusiva de Internet para cualquier host de Internet. Este proceso, denominado "resolución del nombre", utiliza el sistema DNS (sistema de nombres de dominios).
descarga	Datos que se han descargado, por ejemplo de un sitio Web a través de HTTP.

Término	Definición
descargar	Transferir datos o un código de un equipo a otro. A menudo hace referencia a la transferencia desde un sistema host grande (sobre todo un servidor u ordenador central) a un sistema cliente más pequeño.
Preguntas más frecuentes	Preguntas más frecuentes: lista de preguntas y respuestas sobre un tema en concreto.
archivo	Elemento de datos utilizado para fines de almacenamiento, como un mensaje de correo electrónico o una descarga HTTP.
Tipo de archivo	La clase de datos almacenados en un archivo. La mayoría de los sistemas operativos utilizan la extensión del nombre de archivo para determinar el tipo de archivo. El tipo de archivo se suele utilizar para elegir el icono apropiado que representa el archivo en una interfaz de usuario y la aplicación correcta con la que se puede visualizar, editar, ejecutar o imprimir el archivo.
spyware o grayware	Tipo de software que puede ser legítimo, no deseado o malicioso. Al contrario de amenazas como virus, gusanos o troyanos, el grayware ni infecta, ni duplica, ni destruye datos, sino que puede violar su privacidad. El spyware, el adware y las herramientas de acceso remoto son ejemplos de grayware.
gateway	Un gateway o puerta de enlace es un programa o dispositivo de uso específico que transfiere datagramas de IP de una red a otra hasta que se llega al destino final.
GUI	Interfaz gráfica de usuario: uso de imágenes en lugar de únicamente texto para representar la entrada y salida de un programa. Contrasta con la interfaz de línea de comandos, ya que en ésta la comunicación se produce por intercambio de cadenas de texto.
disco duro (o unidad de disco duro)	Uno o más discos magnéticos rígidos que giran alrededor de un eje central, que cuentan con cabezales y sistemas electrónicos de lectura y escritura asociados, y se utilizan para leer y escribir discos duros o disquetes, además de para almacenar datos. Muchos discos duros están conectados de forma permanente a la unidad (discos fijos), si bien también los hay extraíbles.
HTTP	Protocolo de transferencia de hipertexto: protocolo TCP/IP de cliente-servidor que se utiliza en Internet para el intercambio de documentos HTML. Normalmente utiliza el puerto 80.

TÉRMINO	DEFINICIÓN
HTTPS	Protocolo seguro de transferencia de hipertexto: variante de HTTP que se utiliza para realizar transacciones seguras.
host	Equipo conectado a una red.
Internet	Sistema de recuperación de información de hipertexto de cliente-servidor basado en una serie de redes conectadas con routers. Internet es un sistema de información moderno y un medio globalmente aceptado para publicitarse, realizar ventas en línea y ofrecer servicios, así como para establecer redes universitarias y muchas otras redes de investigación. La World Wide Web (red global mundial) es el aspecto más conocido de Internet.
Protocolo de Internet (IP)	Protocolo estándar de Internet que define una unidad básica de datos llamada datagrama. Los datagramas se utilizan en los sistemas de entrega sin conexión "best-effort". El protocolo de Internet define cómo se transfiere la información entre los sistemas por Internet.
intranet	Cualquier red que proporciona dentro de una organización servicios similares a los que proporciona Internet fuera de ella, pero sin necesidad de conectarse a Internet.
IP	Protocolo de Internet: consulte dirección IPv4 o dirección IPv6.
Dirección IPv4	Dirección de Internet de un dispositivo de una red, generalmente expresada con la notación por puntos, como `123.123.123.123`.
Dirección IPv6	Dirección en Internet de un dispositivo incluido dentro de una red; generalmente se indica con una expresión `1234:1234:1234:1234:1234:1234:1234:1234`.
TI	Tecnología de la información, que incluye hardware, software, redes, telecomunicaciones y asistencia técnica.
Archivo Java	Java es un lenguaje de programación de carácter general desarrollado por Sun Microsystems. Un archivo Java contiene código Java. Java es compatible con la programación para Internet en forma de subprogramas Java independientes de la plataforma. (Un subprograma es un programa escrito en lenguaje Java que se puede incluir dentro de una página HTML. Cuando utiliza un explorador habilitado para tecnología Java para visualizar una página que contiene un subprograma, el código de éste se transfiere al sistema y lo ejecuta la máquina virtual Java del explorador.)

Término	Definición
Código malicioso Java	Código vírico escrito o incrustado en Java. Consulte también archivo Java.
Virus JavaScript	JavaScript es un lenguaje de programación sencillo desarrollado por Netscape que permite a los desarrolladores Web agregar contenido dinámico a las páginas HTML que se muestran en un explorador mediante el uso de secuencias de comandos. JavaScript comparte algunas de las características del lenguaje de programación Java de Sun Microsystems, pero se ha desarrollado de forma independiente. Un virus JavaScript es un virus dirigido a estas secuencias de comandos del código HTML. Esto permite al virus residir en las páginas Web y descargarse al escritorio del usuario mediante el explorador. Consulte también virus VBscript.
KB	Kilobyte: 1.024 bytes de memoria.
licencia	Autorización legal para hacer uso del producto de Trend Micro.
enlace (también llamado hiperenlace)	Referencia procedente de algún punto dentro de un documento de hipertexto a otro documento u otro lugar del mismo documento. Normalmente los enlaces se resaltan con un color o estilo de texto diferente, como por ejemplo texto azul subrayado. Al activar el enlace, por ejemplo haciendo clic sobre él con el ratón, el explorador muestra el destino del enlace.
red de área local (LAN)	Cualquier tecnología de red que interconecta recursos dentro de un entorno de oficina, normalmente a alta velocidad, como por ejemplo Ethernet. Una red de área local es una red de corta distancia que se utiliza para conectar un grupo de equipos que se encuentran dentro de un mismo edificio. La red de área local más utilizada es la Ethernet 10BaseT. Como punto de conexión común se utiliza un dispositivo de hardware llamado concentrador, que permite el envío de datos de un equipo a otro dentro de la red. Las LAN están limitadas normalmente a distancias inferiores a 500 metros y ofrecen funciones de red de banda ancha a bajo coste dentro de una zona geográfica pequeña.
malware (software malicioso)	Programas o archivos que se han desarrollado con la finalidad de causar daños, como virus, gusanos o troyanos.
consola de administración	La interfaz de usuario del producto de Trend Micro. También se conoce como la consola del producto.

TÉRMINO	DEFINICIÓN
Mbps	Millones de bits por segundo: medida de ancho de banda en las comunicaciones de datos.
MB	Megabyte: 1.024 kilobytes de datos.
ataque de amenazas mixtas	Ataques complejos que se aprovechan de varios puntos de entrada y vulnerabilidades de las redes de las empresas, como las amenazas "Nimda" o "Código Rojo".
Traducción de direcciones de red (NAT)	Estándar para traducir direcciones IP seguras a direcciones IP registradas, externas y temporales desde el grupo de direcciones. Permite a las redes de confianza con direcciones IP asignadas de forma privada tener acceso a Internet. Esto también implica que no es necesario tener una dirección IP registrada para cada equipo de la red.
Virus de red	Un tipo de virus que utiliza los protocolos de red como TCP, FTP, UDP, HTTP y los protocolos de correo electrónico para replicarse. Generalmente, los virus de red no alteran los archivos del sistema ni modifican los sectores de arranque de los discos duros. En vez de ello, infectan la memoria de los equipos cliente y los obligan a desbordar la red con tráfico, lo que puede originar una ralentización del sistema e incluso el fallo de toda la red.
notificación (Consulte también acción y destino)	Mensaje que se reenvía a uno o más: administrador del sistema, remitente de un mensaje, destinatario de un mensaje, descarga de archivos o transferencia de archivos. El objetivo de la notificación es comunicar que ha tenido lugar o se ha intentado llevar a cabo una acción prohibida, como la detección de un virus en un intento de descarga de archivos HTTP.
sistema operativo	El software encargado de realizar tareas como la interfaz de hardware periférico, la programación de tareas y la asignación de almacenamiento. En los documentos, el término también se refiere al software que presenta un sistema y una interfaz de usuario gráfica en ventanas.
parámetro	Una variable, como un rango de valores (un número del 1 al 10).

Término	Definición
archivo de patrón (también conocido como publicación oficial de patrones)	El archivo de patrón, conocido como publicación oficial de patrones (OPR), es la compilación de patrones más reciente para los virus identificados. Se garantiza que ha pasado una serie de pruebas críticas para garantizar que obtiene la protección óptima frente a las últimas amenazas de virus. Se obtiene su mayor eficacia si se utiliza junto con el motor de escaneo más reciente.
puerto	Canal lógico o punto final de canal de un sistema de comunicaciones que se utiliza para distinguir canales lógicos diferentes de la misma interfaz de red de un mismo equipo. Cada programa de aplicación tiene un número de puerto exclusivo asociado.
proxy	Proceso que ofrece un caché de elementos disponible en otros servidores que son presumiblemente más lentos o más caros para acceder a ellos.
servidor proxy	Un servidor de Internet que acepta las direcciones URL con un prefijo especial que se utiliza para recuperar documentos desde un servidor de caché local o desde un servidor remoto, y que, a continuación, devuelve la URL al solicitante.
Explorar	Examinar en una secuencia determinada los elementos de un archivo para detectar los que coinciden con unos criterios específicos.
motor de exploración	El módulo que realiza la exploración antivirus y la detección en el producto host en el que está integrado.
sector	Porción física de un disco. (Consulte también partición, que es una porción lógica de un disco.)
SSL (Capa de conexión segura)	La capa de conexión segura (SSL) es un protocolo diseñado por Netscape para ofrecer capas de seguridad de los datos entre los protocolos de las aplicaciones (como HTTP, Telnet o FTP) y TCP/ IP. Asimismo, ofrece opciones como el cifrado de datos, la autenticación del servidor, la integridad de los mensajes y autenticación cliente opcional para una conexión TCP/IP.

TÉRMINO	DEFINICIÓN
servidor	Un programa que ofrece un servicio a otros programas (cliente). La conexión entre el cliente y el servidor se suele realizar mediante la transmisión de mensajes, a menudo a través de una red, y utiliza algún protocolo para cifrar las solicitudes del cliente y las respuestas del servidor. El servidor se puede ejecutar de forma continua (como un demonio), esperando peticiones de llegada, o puede que lo invoque algún demonio de alto nivel que controle un número determinado de servidores.
unidad compartida	Dispositivo periférico de los equipos que lo utilizan más de una persona, por lo que aumenta el riesgo de exposición a virus.
firma	Consulte firma de virus.
SNMP	Protocolo simple de administración de red: protocolo compatible con la supervisión de los dispositivos adjuntos a una red en condiciones que merecen atención administrativa.
trafico	Flujo de datos entre Internet y la red, tanto datos de entrada como de salida.
Protocolo de control de transmisión/ Protocolo de Internet (TCP/IP)	Protocolo de comunicaciones que permite a los equipos con diferentes sistemas operativos comunicarse entre ellos. Controla cómo se transfieren los datos de Internet entre los equipos.
provocar	Acontecimiento que hace que se lleve a cabo una acción. Por ejemplo, el producto de Trend Micro detecta un virus en un mensaje de correo electrónico. Esto puede provocar que el mensaje se ponga en cuarentena y que se envíe una notificación al administrador del sistema y al remitente y al destinatario del mensaje.
tipo de archivo verdadero	Lo utiliza IntelliScan, una tecnología de exploración de virus, para identificar de qué tipo es la información de un archivo mediante la exploración de sus encabezados, independientemente de la extensión del nombre del archivo (que podría ser engañosa).
URL	Localizador universal de recursos: forma estándar de especificar la ubicación de un objeto, normalmente una página Web, en Internet, como por ejemplo: www.trendmicro.com. La dirección URL se asigna a una dirección IP mediante DNS.

Término	Definición
dirección IP virtual (dirección VIP)	Una dirección VIP asigna el tráfico recibido en una dirección IP a otra dirección basada en el número de puerto de destino del encabezado del paquete.
Red de área local virtual (VLAN)	Agrupación lógica (en lugar de física) de dispositivos que forman un dominio de transmisiones único. Los miembros de una VLAN no se identifican por su ubicación en una subred física sino mediante el uso de etiquetas en los encabezados de los marcos de los datos transmitidos. Las VLAN se describen en el estándar IEEE 802.1Q.
Red privada virtual (VPN)	Una VPN es una forma fácil, rentable y segura que tienen las empresas de ofrecer a los teletrabajadores y a los profesionales móviles acceso de marcación local a su red corporativa o a otro proveedor de servicios de Internet (ISP). Las conexiones privadas seguras en Internet resultan más rentables que las líneas privadas dedicadas. Las VPN son posibles gracias a tecnologías y estándares como el tunelado y el cifrado.
router virtual	Un router virtual es el componente de Screen OS que lleva a cabo funciones de enrutamiento.
sistema virtual	Un sistema virtual es una subdivisión del sistema principal que parece ser una entidad autónoma para el usuario. Los sistemas virtuales residen separados unos de otros en el mismo dispositivo remoto GateLock de Trend Micro. Cada uno de ellos lo puede administrar su propio administrador del sistema virtual.
virus	Un virus informático es un programa (un fragmento de código ejecutable) con la exclusiva habilidad de infectar. Al igual que los virus biológicos, los virus informáticos pueden propagarse rápidamente y a menudo es difícil erradicarlos. Además de replicarse, algunos virus informáticos comparten otra característica común: una rutina de daños que transmite la acción destructiva del virus. Aunque algunas rutinas de daños pueden consistir en mostrar solo un mensaje o una imagen, también pueden destruir archivos, formatear el disco duro y causar otro tipo de daños. Aunque el virus no contenga una rutina de daños, puede causar problemas, ya que consume espacio de almacenamiento y memoria, y puede degradar el rendimiento general del equipo.
Web	La red global mundial, también llamada la Web o Internet.

TÉRMINO	DEFINICIÓN
Servidor Web	Un proceso de servidor que se ejecuta en un sitio Web que envía páginas en respuesta a las solicitudes HTTP realizadas desde exploradores remotos.
estación de trabajo (también conocida como cliente)	Equipo de uso general que está diseñado para que se utilice de forma individual y que ofrece un rendimiento superior al que normalmente ofrece un ordenador personal, sobre todo en lo que se refiere a gráficos y capacidad de procesamiento y de llevar a cabo diversas tareas al mismo tiempo.

Índice

C

componentes, 3-6
convenciones del documento, vii

L

Lista de bloqueo Web, 1-4

P

pantalla de resumen
    componentes, 3-6
    pestañas, 3-3
pestañas, 3-3

S

Smart Protection Network, 1-3
Smart Protection Server, 1-3
Smart Scan Agent pattern, 1-4
Smart Scan pattern, 1-4
soporte
    base de conocimientos, 4-2
    resolver los problemas más rápido, 4-5
    TrendLabs, 4-5

T

TrendLabs, 4-5
Trend Micro
    acerca de, vi

TREND MICRO INCORPORATED

TREND MICRO España Plaza de las Cortes, 4 – 8º Izq. Madrid, 28014 España

Teléfono: +34 91 369 70 30 Fax: +34 91 369 70 31 reception_es@trendmicro.es

www.trendmicro.com

Item Code: APEM36294/140116